(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 903 886 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
24.03.1999 Bulletin 1999/12

(51) Int. Cl.^{6}: H04L 9/00

(21) Application number: 98117568.0

(22) Date of filing: 16.09.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 18.09.1997 JP 253158/97

(71) Applicant:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.
Kadoma-shi, Osaka-fu (JP)

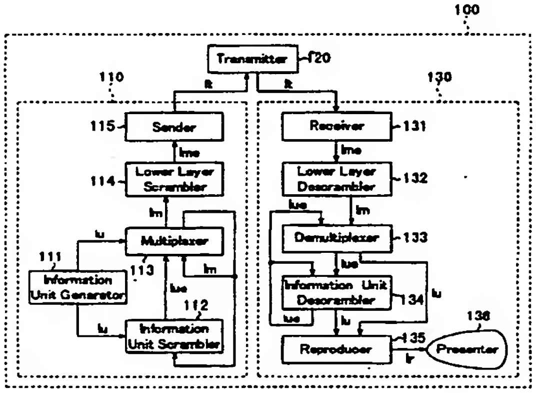
(72) Inventors:
- Kataoka, Mitsuteru
Fujisawa-shi, Kanagawa-ken (JP)
- Harada, Takenosuke
Yokohama-shi, Kanagawa-ken (JP)
- Machida, Kazuhiro
Inzai-shi, Chiba-ken (JP)
- Masuda, Isao
Tokyo-to (JP)

(74) Representative:
Altenburg, Udo, Dipl.-Phys. et al
Patent- und Rechtsanwälte
Bardehle - Pagenberg - Dost - Altenburg -
Geissler - Isenbruck,
Gallileiplatz 1
81679 München (DE)

(54) Information transmission method and apparatus for combining multiplexing and encryption

(57) An information transmission system (100) transmits an encrypted information (It) comprised of a plurality of information units (Iu) each hierarchically encrypted and multiplexed to each other is communicated between at least two parties. The information transmission system (100) is constructed by a transmitting unit (110) and a receiving unit (130). The transmitting unit (110) is provided with an information unit generator (111) which produces the information unit (Iu); a scrambler (112) which encrypts the information unit (Iu) to produce an encrypted information unit (Iue), and multiplexer (113) which multiplexes at least one of those information unit (Iu) and said encrypted information unit (Iue) to produce a multiplexed information unit (Im). The receiving unit (130) is provided with a lower layer descrambler (132) which decrypts the encrypted information (It) to produce a multiplexed information unit (Im), demultiplexer (133) which demultiplexes the multiplexed information unit (Im) into any of encrypted information unit (Iue), multiplexed information unit (Iue) and information unit (Iu), and information unit descrambler (134) which decrypts the encrypted information unit (Iue) .

Fig. 1



EP 0 903 886 A2

Printed by Xerox (UK) Business Services
2.16.7/3 6

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates generally to a method and an apparatus for encrypting information in computer communication and data broadcasting, and transmitting the encrypted information.

Description of the Background Art

[0002] In Fig. 25, a conventional information transmission apparatus is shown. The conventional information transmission apparatus 1900 includes a transmitting unit 1910, transmitter 1920, and receiving unit 1930. Description is now made by taking two types of specific examples, those are information transmission in the Internet as Example 1 and digital broadcasting as Example 2. A plurality of receiving units 1930 may correspond to one transmitting unit 1930.

[0003] The transmitting unit 1930 produces transmission information It obtained by subjecting an information unit Iu to multiplexing and encryption, and output thereof. The information unit Iu is a collection of electronic data having meanings for a user, for example, such as text information, voice information, still image information, moving image information, HTML (Hypertext Makeup Language) information, and their combination.

Transmitting unit 1910

[0004] The transmitting unit 1910 contains an information unit generator 1911, a multiplexer 1912, a lower layer scrambler 1913, and a sender 1914.

[0005] The information unit generator 1911 generates a plurality of information units Iu, and outputs thereof. In Example 1, the information unit generator 1911 outputs the information units Iu which are, for example, a text the user entered with a keyboard or the like, and an image taken into a computer, and others already stored in the computer. The information unit generator 1911 is an input screen portion of electronic mail software, and a server in a broadcasting station on the Internet, for example.

[0006] On the other hand, in Example 2, all information units Iu generated are previously stored in the information unit generator 1911. A method for merely selectively outputting the information units Iu in accordance with a predetermined schedule is considered. The information unit generator 1911 is a broadcasting station system containing a program management system in a sending system of digital broadcasting, a cart machine of a VTR, an MPEG-2 encoder, an EPG (Electronic Program Guide) management sending system of digital broadcasting, and the like. Additional information such as EPG must be sent out with the same contents thereof maintained for a long time. Therefore, the same contents may, in some cases, are repeatedly outputted in a period on the order of seconds in the information unit generator 1911.

[0007] The multiplexer 1912 receives the plurality of information units Iu outputted by the information unit generator 1911. Then, the multiplexer 1912 multiplexes the inputted information units Iu, and outputs the multiplexed information units Iu as multiple information Im. By the multiplexing, the plurality of information units Iu are converted into a format (multiple information Im) suitable for efficient transmission in the transmitter 1920.

[0008] In Example 1, the multiplexer 1912 is an MIME (Multi-purpose Internet Mail Extensions) encoder used for sending multimedia information by an electronic mail on the Internet, for example. In this case, the multiplexer 1912 respectively takes text information, image information, voice information, and so forth which are the plurality of information units Iu as parts. Then the multiplexer 1912 converts the parts into a multipartite message conforming to MIME for collecting the plurality of parts, and outputs the message. The formal specification of the MIME is defined by RFC (Request for Comments) 1521/1522.

[0009] On the other hand, in Example 2, the multiplexer 1912 is a service multiplexer for obtaining TS (Transport Stream) of an MPEG-2 systems from a plurality of stream data, for example. The MPEG-2 systems and the TS are standardized by ISO/IEC CD 13818-1. In this case, the multiplexer 1912 divides each of the plurality of information units Iu outputted by the information unit generator 1911 into packets called PES (Packetized Elementary Stream), and multiplexes the obtained packets on the basis of a certain rule.

[0010] The lower layer scrambler 1913 receives the multiple information Im outputted by the multiplexer 1912, and encrypts the multiple information Im in accordance with a predetermined encryption algorithm, and outputs the encrypted result as encrypted multiple information Ime. In Example 1, the lower layer scrambler 1913 may be software PGP (Pretty Good Privacy) on which an RSA cipher which is a public key cipher, for example, mounted therein is started with an encryption option. An output of the lower layer scrambler 1913 is a text of an electronic mail encrypted using the RSA cipher. The RSA cipher is described in detail in an article entitled by R. L. Rivest, A. Shamir, and L. Adleman which are contrivers themselves "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" (Vol. 21, No. 2 issued on February, 1978 in Communications of the ACM). The PGP is described in detail in an article entitled by Simson Garfinkel "PGP: Pretty Good Privacy" (O'Reilly & Associates).

[0011] On the other hand, in Example 2, the lower layer scrambler 1913 may be, for example, a scrambler of a transport layer. The lower layer scrambler 1913 encrypts a payload portion of inputted TS of MPEG-2 using an encryption algorithm such as MULTI2 and DES(the Data Encryption Standard), and outputs the encrypted TS of the MPEG-2 which is the result thereof. Note that MULTI2 described in ARIB report No. 74 is developed by Hitachi Ltd. for the application of digital broadcasting system.

[0012] The sender 1914 receives the encrypted multiple information Ime outputted by the lower layer scrambler 1913, and converts the encrypted multiple information Ime into transmission information It which will be inputted to the transmitter 1920. In Example 1, the sender 1914 is a program for adding a mail header composed of a destination field, a sender field, and so forth to the text of the electronic mail. An output of the sender 1914 is the text of the electronic mail to which the mail header is added. On the other hand, in Example 2, the sender 1914 is an error-correcting encoder and a modulator for the TS of the MPEG-2.

Transmitter 1920

[0013] The transmitter 1920 transmits the inputted transmission information It to a physically distant point. Both inputs and outputs of the transmitter 1920 are the transmission information It. All the inputs of the transmitter 1920 may not appear in the outputs to the receiving unit 1930 without any error. In Example 1, the transmitter 1920 is a plurality of mail communication daemons which are connected to each other by a channel such as the Internet for interpreting and executing an SMTP (Simple Mail Transfer Protocol). Examples of the typical mail communication daemon include "sendmail". The formal specification of the SMTP is defined by RFC 821, RFC 822, and RFC 974. The sendmail is described in detail in an article entitled by E. Allman ""SENDMAIL - An Internetwork Mail Router" Unix Programmer's manual" (CSRG U. C. Berkeley issued on July, 1983).

[0014] On the other hand, in Example 2, the transmitter 1920 is constituted by an up-converter, a parabola antenna for sending data to a satellite, a communication satellite, and a ground receiving antenna.

Receiving unit 1930

[0015] The receiving unit 1930 receives the transmission information It transmitted by the transmitter 1920, and presents an information unit Iu to a user. The receiving unit 1930 includes a receiver 1931, a lower layer descrambler 1932, a demultiplexer 1933, a reproducer 1934, a storage 1935, and presenter 1936.

[0016] The receiver 1931 receives the transmission information It outputted by the transmitter 1920, and takes out the whole or a part of thereof. Then, the receiver 1931 reproduces an encrypted multiple information Ime based on the transmission information It taken out. In Example 1, the receiver 1931 is a front end program for mail transmission. On the other hand, in Example 2, the receiver 1931 is the connection of a satellite broadcasting tuner, a demodulator and an error-correcting decoder.

[0017] The lower layer descrambler 1932 receives the encrypted multiple information Ime outputted by the receiver 1931, and decrypts the encrypted multiple information Ime, and reproduces the multiple information Im. In Example 1, the lower layer descrambler 1932 is a PGP program which is started with a decryption option. On the other hand, in Example 2, the lower layer descrambler 1932 is a descrambler of the transport layer.

[0018] The demultiplexer 1933 separates each information unit Iu from the multiple information Im, takes out the separated information unit Iu, and outputs the information unit Iu taken out. In Example 1, the demultiplexer 1933 is an MIME decoder, and separates the text information, the image information, and so forth which are then respective parts included in the multipartite message as separate information, to take out the separate information. On the other hand, in Example 2, the demultiplexer 1933 is a demultiplexer for the TS of the MPEG-2. The demultiplexer 1933 separates a plurality of streams which are multiplexed by the MPEG-2 systems.

[0019] The reproducer 1934 receives the information unit Iu outputted by the demultiplexer 1933, and produces a reproduction information Ir1 which is reproducible information. In Example 1, the reproducer 1934 may be a text file viewer, image file presenting software, etc. On the other hand, in Example 2, the reproducer 1934 may be an MPEG-2 decoder for reproducing voices or images encoded by the MPEG-2, for example. In this case, the output is an NTSC (National Television System Standard Committee) signal or an analog voice signal.

[0020] The storage 1935 receives the reproduction information outputted by the reproducer 1934, and stores the first reproduction information Ir1. Then, the storage 1935 also outputs the first reproduction in formation Ir1 therefrom as a second reproduction information Ir2 on demands for reproduction. This operation is hereinafter merely referred to as "reproduction". It is to be noted that the first and second reproduction information Ir1 and Ir2 are identical with respect to the contents thereof, but different in time for the presentation, as described soon later.

[0021] In Example 1, the storage 1935 may be a file system in OS (operating System) or software for managing the classification of electronic mails. On the other hand, in Example 2, the storage 1935 may be a VTR (Video Tape Recorder) or VCR (Video Cassette Tape Recorder) for recording and reproducing an NTSC signal and an analog voice signal.

[0022] The presenter 1936 receives the first reproduction information Ir1 and outputted by the reproducer 1934 and the second reproduction information Ir2 outputted by the storage 1935, and presents either one or both of the information to a user. In Example 1, the presenter 1936 may be a window system such as X-window or Microsoft Windows for presenting image and voice to a user. On the other hand, in Example 2, the presenter 1936 may be a television receiver for inputting and receiving an NTSC signal and an analog voice signal, for example.

[0023] In Fig. 26, an example of encrypted multiple information unit Ime0d produced by the information transmission apparatus 1900 is shown. According to this example, the encrypted multiple information unit Ime0d includes four information units Iu1d, Iu2d, Iu3d, and Iu4d each indicated by a circle in the drawing. A rectangle indicated by a dot line represents an encrypted multiple information unit Ime obtained by encrypting the information units Iu1d, Iu2d, Iu3d, and Iu4d once in the lower layer scrambler 1913. In other words, all the information units Iu1d, Iu2d, Iu3d, and Iu4d are encrypted with the same cipher, and are protected by the single encryption layer in the transportation level.

[0024] The information units Iu1d, Iu2d, Iu3d, and Iu4d represents a tourist resort guide considering the weather forecast, a weather forecast for the tourist resorts, a weather forecast for allover the country, and a weather forecast for a local area, respectively. These sub-tiles with respect to weather forecast are encrypted to generate a total weather forecast program Iue. Thus, there is no hierarchical order among these sub-tiles from the view point of encryption.

In Operation

[0025] With reference to Figs. 27 and 28, the operation of the conventional information transmission apparatus 1900 is described below. In Fig. 27, a flow chart showing the operation performed by the transmitting unit 1910 and the transmitter 1920 is shown.

[0026] At step S2001, the information unit generator 1911 generates a plurality of information units Iu, and outputs the generated information units Iu. Examples of the generation of the information units Iu include a method in which a user enters information units Iu and designates a file as in Example 1, and a case where information units Iu are selectively outputted from stored information units Iu in accordance with a predetermined schedule as in Example 2.

[0027] At step S2002, the multiplexer 1912 multiplexes the information units Iu generated at step S2001, and outputs the result thereof as multiple information Im. The multiple information Im is multipartite data conforming to the MIME in the case of Example 1, while being data representing the TS of the MPEG-2 systems in the case of Example 2.

[0028] At step S2003, the lower layer scrambler 1913 encrypts the multiple information Im obtained by the multiplexing at step S2002, and produces the encrypted multiple information Ime. In Example 1, the multiple information Im is encrypted using the RSA cipher or the like. On the other hand, in Example 2, the payload portion of the TS of the MPEG-2 is encrypted using a MULTI2 cipher manufactured by Hitachi Ltd., for example.

[0029] At step S2004, the sender 1914 converts the encrypted multiple information Ime obtained by the encryption at step S2003 into a format which is transmittable or suitable for transmission by the transmitter 1920, and produces the transmission information It. In Example 1, information obtained by adding information, for example, "To : " field, "From : " field to the head of the text of the mail which is encrypted multiple information Ime is outputted as transmission information It. On the other hand, in Example 2, information obtained by encoding the TS of the MPEG-2 using an error-correcting code and then, modulating the encoded TS is outputted.

[0030] At step S2005, the transmitter 1920 transmits the transmission information It to a physically distant point. In Example 1, the mail communication daemons mounted on one or a plurality of computers connected are communicated to a computer network such as the Internet or a LAN (Local Area Network) on the basis of the SMTP. Thus, the mail is transmitted from the mail communication daemon on one of the computers to the mail communication daemon on the other computer.

[0031] On the other hand, in Example 2, transmission information It obtained by the conversion in the up-converter is transmitted to the communication satellite by the parabolic antenna. The communication satellite transmits the received transmission information It to the ground by a transponder. The transmission information It from the communication satellite is received by the ground receiving antenna.

[0032] With reference to Fig. 28, the operation performed by the receiving unit 1930 is described, here below. In Fig. 28, the operations of taking out an information unit Iu in real time from the transmission information It, presenting the information unit Iu to the user, storing the information unit Iu as required by the user, and later viewing the information unit Iu again are specifically shown.

[0033] At step S2101, when the user views the information unit Iu in real time from the transmission information It, the procedure advances to step S2102. When the user views the information unit Iu previously stored in the storage 1935, the procedure advances to step S2109.

[0034] At step S2102, the receiver 1931 receives the transmission information It from the transmitter 1920, and takes out a part or the whole of the encrypted multiple information Ime from the inputted transmission information It. In Example 1, processing for taking out one electronic mail data addressed to a specific user is performed. On the other hand, in Example 2, processing for filtering a particular packet storing information to be found by a PID (Packet ID), and selecting and extracting the packet is performed by tuning to a predetermined frequency.

[0035] At step S2103, the lower layer descrambler 1932 receives the encrypted multiple information Ime outputted by the receiver 1931, and decrypts the encrypted multiple information Ime, and outputs multiple information Im. In Example 1, the lower layer descrambler 1932 is the PGP program started with a decryption option. Decryption is performed using the RSA cipher by the PGP program, and the result of the decryption is outputted. On the other hand, in Example 2, th.. multiple information Im encrypted using the MULTI2 cipher is decrypted, to obtain multiple information Im.

[0036] At step S2104, the demultiplexer 1933 separates each information unit Iu from the multiplexed information units Im and takes out the information unit Iu. In Example 1, the demultiplexer 1933 separates for each part the multipartite message obtained by multiplexing on the basis of the MIME. As a result, the text information, the image information, the voice information, and so forth which are the respective parts are separated as discrete information units Iu.

[0037] On the other hand, in Example 2, the demultiplexer 1933 separates the plurality of streams multiplexed by the MPEG-2 systems on the basis of a PID (Packet ID, a packet identifier). As a result, additional information such as an MPEG-2 video stream, an MPEG-1 audio stream, and EPG are separated as discrete information units Iu. An MPEG-2 video is standardized by ITU-T H. 262, and a MPEG-1 audio is standardized as ISO/IEC 11172-3 Standard.

[0038] At step S2105, the reproducer 1934 receives the information unit Iu outputted by the demultiplexer 1933, and produces the first reproduction information Ir1 which is reproducible information. In Example 1, when the information unit Iu is text information, for example, fonts corresponding to respective character codes are selected and listed, to generate a bitmap format as the reproduction information Ir1. When the information unit Iu is in an image information format such as JPEG (Joint Photographics Experts Group), it is expanded into the bitmap format, and the result of the expansion is outputted as reproduction information. The JPEG is standardized by ISO/IEC 10918. When the information unit Iu is voice information, it is converted into an analog voice signal by the same function as that of a digital-to-analogue (D/A) converter. And the analog voice signal is also outputted as reproduction information.

[0039] On the other hand, in Example 2, when the information unit Iu obtained at step S2104 is the MPEG-2 video stream, the MPEG-2 video is decoded, and outputs the NTSC signal as reproduction information. When the information unit Iu is a voice stream, it is converted into an analog voice signal by D/A conversion, and the analog voice signal is outputted.

[0040] At step S2106, the presenter 1936 presents the first reproduction information Ir1 obtained at step S2105 to the user in accordance with the format of the reproduction information. In Example 1, when the reproduction information obtained at step S2105 is in the bitmap format, the presenter 1936 arranges and presents the reproduction information Ir1 on a display screen. Thus, the reproduction information Ir1 is presented to the user. When the reproduction information obtained at step S2105 is an analog voice signal, the analog voice signal is converted into sound by being sent to a speaker, and is visually presented to the user.

[0041] On the other hand, in Example 2, an NTSC signal as the reproduction information which is obtained at step S2105 is received on a display, the analog voice information is sent to a speaker, and the reproduction information is presented to the user.

[0042] At step S2107, the procedure advances to step S2108 in a case where an attempt to store information in the current transmission information It is made by presenting the intention of the user, while proceeding to step S2101 in the other case. Specific examples of a case where the intention of the user is presented include a case where it is designated while being viewed and a case where it is previously set by a timer or the like.

[0043] At step S2108, the reproduction information generated at step S2105 is stored in the storage 1935. Thereafter, the procedure advances to step S2101. Reproduction information Ir1 may be additionally stored in the storage 1935, or the information Ir1 already stored may be overwritten by the additionally stored information Ir1. Alternatively, in a case where information with an old version has been already stored in the storage 1935, the information with an old version may be replaced.

[0044] In Example 1, the reproduction information is stored and arranged in a file system. The information units Iu are arranged in the order of arrival, by sending person, and by topic, for example. On the other hand, in Example 2, the reproduction information such as images and voices is recorded on a video tape or the like. For example, additional information other than images and voices which are multiplexed in a NTSC vertical blanking period may be simultaneously stored. In a case where digital information is recorded as it is, a plurality of streams other than images and voices may be simultaneously recorded.

[0045] At step S2109, the first reproduction information Ir1 stored in the storage 1935 is outputted therefrom as the second reproduction information Ir2. In Example 1, the reproduction information Ir2 (Ir1) selected by the user out of the reproduction information Ir1 arranged and stored in the file system is outputted. On the other hand, in Example 2, images and voices are reproduced from the video tape or the like. Although the selection of the reproduction information Ir2 (Ir1) which the user desires to select may be automated by being realized as the function of the storage 1935, the user himself or herself may also selects the video tape or the like and set the selected video tape in the storage 1935.

[0046] At step S2110, the presenter 1936 presents the reproduction information outputted at step S2109 to the user. Thereafter, the procedure returns to step S2101. The operation at step S2110 may be the same as that at step S2106 except that the procedure returns to step S2101.

[0047] However, as described in the above, the conventional information transmission apparatus 1900 faces to the following two main problems. The first problem is that there is a restriction on the degree of freedom to setting the resistance of a cipher against unfair decryption. In general, the higher the resistance of the cipher to unfair decryption is, the more resources such as computer resources and processing time are required for decryption processing performed by a fair decrypting method. Therefore, encryption using a cipher having necessary and sufficient resistance is required depending on secrecy required of an object to be encrypted.

[0048] For example, when encryption higher in secrecy is required of an information unit Iu which is a part of information to be transmitted, the information unit Iu which is the part must be subjected to encryption using a cipher having higher resistance. For example, when in a weather forecast program, a weather forecast for allover the country is free and is not encrypted. However, a detailed forecast for the local area is charged, and a weather forecast custom-maid for each user is charged extra. Therefore, the detailed forecast for the local area must be subjected to encryption higher in secrecy than the weather forecast for allover of the country, and the custom-made weather forecast must be subjected to encryption higher in secrecy than the detailed forecast for the local area.

[0049] Although in many of ciphers, the resistance of the cipher can be theoretically adjusted by increasing the size of a key of cryptanalysis, the resistance of the cipher does not necessarily have a sufficient degree of freedom due to the restriction on hardware for decryption generally used, for example.

[0050] When the hardware for decryption using a cipher having an increased degree of freedom is used, however, some disadvantages occur. For example, a receiving unit 1930 becomes complicated, and special hardware must be prepared. In a case where a key is changed for information units Iu encrypted using ciphers which differ in resistance, encryption and decryption must be performed for each information unit Iu in the worst case, which is not efficient.

[0051] The second problem is that the information unit Iu must be decrypted before it is stored. In general, when charged information is sent in a media which can be accessed by all people, for example, such as broadcasting. In such a charged broadcasting, information is transmitted in an encrypted state in a transmitting unit 1910, and fees are charged at the time point where the information is decrypted in a receiving unit 1930 in many cases. This is for preventing unfair viewing of users who do not pay fees.

[0052] It is necessary for the conventional information transmission apparatus 1900 to store the reproduction information Ir which is generated by decrypting the transmission information It produced by encrypting the information unit Iu sent from the transmitting unit 1910 before the user views the information unit Iu not in real time but some time after transmission. Let consider a case where information units Iu which may be viewed are previously stored and are later viewed.

[0053] When a relatively large number of information units Iu which may be later viewed are stored, some of the information units Iu are not eventually viewed even if they have been decrypted from the transmission information It. In a case where fees are charged at the same time that the information units Iu are descrambled when they are stored, it is disadvantageous for a user. Conversely, when a relatively small number of information units Iu which are to be always later viewed are carefully selected and stored, an information unit Iu cannot be viewed even when a user desires to view the information unit Iu later because it is not stored. The reason for this is that generally it is significantly difficult for the user himself or herself to previously determine which of the information units Iu will be later viewed.

[0054] On the other hand, a method of changing the structure of the receiving unit and storing transmission information It as it is also considered. In this method, when a additional information such as EPG having the same content are repeatedly sent, such information is overlapped with each other. Furthermore, the information units Iu including old and new contents are both stored regardless the version thereof, even though the newest one of them, for example, the number of survivors in a plane accident and software whose version is updated, is worthwhile. Therefore, the capacity of the storage is wasted, which is not realistic, and excess processing is required in taking out the newest information unit Iu.

SUMMARY OF THE INVENTION

[0055] The present invention has been made to solve the above-described conventional problems. At first aspect of the present invention, an information transmission apparatus in use for an information transmission system where an encrypted information comprised of a plurality of information units each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, the information being encrypted for the transmission, the apparatus comprises:

an information unit generator for producing the information unit;

a first encryption unit for encrypting the information unit with a first predetermined encryption system to produce an encrypted information unit; and

a first multiplexer for multiplexing at least one of the information unit and the encrypted information unit to produce a multiplexed information unit.

[0056] As apparently from the above, according to the first aspect of the present invention, it is possible to produce the encrypted information comprised of a plurality of information units which are hierarchically encrypted and multiplexed to each other in various combination.

[0057] According to a second aspect, in the first aspect of the present invention, an information transmission apparatus further comprises:

a second encryption unit for encrypting the multiple information with a second predetermined encryption system to produce the encrypted multiplexed information; and

a second multiplexer for multiplexing the encrypted information unit to produce the multiplexed information.

[0058] As apparently from the above, according to the second aspect of the present invention, it is possible to encrypt each of information units with different encryption system, ensuring the encryption resistance against unfair access the information.

[0059] According to a third aspect, in the second aspect of the present invention, an information transmission apparatus further comprises:

a third encryption unit for encrypting the multiplexed information with a third predetermined encryption system to produce an encrypted multiple information unit.

[0060] According to a fourth aspect, in the third aspect of the present invention, an information transmission apparatus, wherein the third predetermined encryption system is the same as that applied to the encrypted information.

[0061] According to a fifth aspect, in the third aspect of the present invention, an information transmission apparatus, where in the second predetermined encryption system is the same as the third predetermined encryption system.

[0062] According to a sixth aspect, in the third aspect of the present invention, an information transmission apparatus, where in the first, second, and third predetermined encryption systems are the same.

[0063] According to a seventh aspect, in the first aspect of the present invention, an information transmission apparatus further comprises:

a transmitter for converting the encrypted multiplexed information into a format suitable for an efficient transmission.

[0064] According to an eighth aspect, in the first aspect of the present invention, an information transmission apparatus, wherein the first encryption unit encrypts the information unit with an encryption system suitable for the transmission of information.

[0065] According to an eighth aspect, an information transmission apparatus in use for an information transmission system where an encrypted information comprised of a plurality of information units each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, the information being encrypted for the transmission, the apparatus comprising:

a first decryption unit for decrypting the encrypted information with a first decryption system to produce a first multiplexed information unit;

a first demultiplexer for demultiplexing the first multiplexed information unit into any of a first encrypted information unit, a second multiplexed information unit and the information unit; and

a second decryption unit for decrypting the first encrypted information unit with a second decryption system to produce the information unit or a second encrypted information unit.

[0066] According to a tenth aspect, in the ninth aspect of the present invention, an information transmission apparatus further comprising:

a second demultiplexer for demultiplexing the second multiplexed information unit;

a third decryption unit for decrypting the second encrypted information unit with a third predetermined decryption system to produce the information unit.

[0067] According to an eleventh aspect, in the ninth aspect of the present invention, an information transmission apparatus, wherein the first decryption system is the same as that applied to the encrypted information.

[0068] According to a twelve aspect, in the first aspect of the present invention, an information transmission apparatus further comprises:

a storage provided between the first demultiplexer and the second decryption unit for storing any of the first and second encrypted information units.

[0069] According to a thirteenth aspect, in the twelve aspect of the present invention, an information transmission apparatus further comprises:

a reproducer for receiving the encrypted information units from the second decryption unit to produce a reproduction information indicating a content the encrypted information, the reproducer requesting the storage to supply the stored encryption information unit to the second decryption unit.

[0070] According to a fourteenth aspect of the present invention, an information transmission method for transmitting an encrypted information comprised of a plurality of information units each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, the information being encrypted for the transmission, the method comprising the steps of:

producing the information unit;
encrypting the information unit with a first predetermined encryption system to produce an encrypted information unit; and
multiplexing at least one of the information unit and the encrypted information unit to produce a multiplexed information unit.

[0071] As apparently from the above, according to the fourteenth aspect of the present invention, it is possible to produce the encrypted information comprised of a plurality of information units which are hierarchically encrypted and multiplexed to each other in various combination.

[0072] According to a fifteenth aspect, in the fourteenth aspect of the present invention, an information transmission method further comprising the steps of:

encrypting the multiple information with a second predetermined encryption system to produce the encrypted multiplexed information; and
multiplexing the encrypted information unit to produce the multiplexed information.

[0073] As apparently from the above, according to the fourteenth aspect of the present invention, it is possible to encrypt each of information units with different encryption system, ensuring the encryption resistance against unfair access the information.

[0074] According to a sixteenth aspect, in the fifteen aspect of the present invention, an information transmission method further comprises:

encrypting the multiplexed information with a third predetermined encryption system to produce an encrypted multiple information unit.

[0075] According to a seventeenth aspect, in the sixteenth aspect of the present invention, an information transmission method, wherein the third predetermined encryption system is the same as that applied to the encrypted information.

[0076] According to an eighteenth aspect, in the sixteenth aspect of the present invention, an information transmission method, wherein the second predetermined encryption system is the same as the third predetermined encryption system.

[0077] According to a nineteenth aspect, in the sixteenth aspect of the present invention, an information transmission method, wherein the first, second, and third predetermined encryption systems are the same.

[0078] According to a twentieth aspect, in the fourteenth aspect of the present invention, an information transmission method further comprising the step of:

converting the encrypted multiplexed information into a format suitable for an efficient transmission.

[0079] According to a twenty first aspect, in the fourteenth aspect of the present invention, an information transmission method, wherein at the encrypting step the information unit is encrypted with an encryption system suitable for the transmission of information.

[0080] According to a twenty second aspect of the present invention, an information transmission method for transmitting an encrypted information comprised of a plurality of information units each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, the information being encrypted for the transmission, the method comprising the steps of:

decrypting the encrypted information with a first decryption system to produce a first multiplexed information unit;
demultiplexing the first multiplexed information unit into any of a first encrypted information unit, a second multiplexed information unit and the information unit; and
decrypting the first encrypted information unit with a second decryption system to produce the in format ion unit or a second encrypted information unit.

[0081] According to a twenty third aspect, in the twenty second aspect of the present invention, an information transmission method further comprising the steps of:

demultiplexing the second multiplexed information unit;
decrypting the second encrypted information unit with a third predetermined decryption system to produce the information unit.

[0082] According to a twenty fourth aspect, in the twenty second aspect of the present invention, an information transmission apparatus, wherein the first decryption system is the same as that applied to the encrypted information.

[0083] According to a twenty fifth aspect, in the fourteenth aspect of the present invention, an information transmission apparatus further comprising the step of:

storing any of the first and second encrypted information units.

[0084] According to a twenty sixth aspect, in the twenty fifth aspect of the present invention, an information transmission apparatus further comprising the step of:

a reproducer for receiving the encrypted information units from the second decryption unit to produce a reproduction information indicating a content the encrypted information, the reproducer requesting the storage to supply the stored encryption information unit to the second decryption unit.

[0085] According to a twenty seventh aspect of the present invention, an information transmission system for transmitting an encrypted information comprised of a plurality of information units each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, the information being encrypted for the transmission, the system comprises:

an information unit generator for producing the information unit;
a first encryption unit for encrypting the information unit with a first predetermined encryption system to produce an encrypted information unit;
a first multiplexer for multiplexing at least one of the information unit and the encrypted information unit to produce a multiplexed information unit;
a first decryption unit for decrypting the encrypted information with a first decryption system to produce a first multiplexed information unit;
a first demultiplexer for demultiplexing the first multiplexed information unit into any of a first encrypted information unit, a second multiplexed information unit and the information unit; and
a second decryption unit for decrypting the first encrypted information unit with a second decryption system to produce the information unit or a second encrypted information unit.

[0086] As apparently from the above, according to the twenty seventh aspect of the present invention, it is possible to produce the encrypted information comprised of a plurality of information units which are hierarchically encrypted and multiplexed to each other in various combination. It is also possible to reproduce the information from thus hierarchically encrypted and multiplexed information.

[0087] According to a twenty eighth aspect, in the twenty seventh aspect of the present invention, an information transmission system further comprises:

a second encryption unit for encrypting the multiple information with a second predetermined encryption system to produce the encrypted multiplexed information; and
a second multiplexer for multiplexing the encrypted information unit to produce the multiplexed information.

[0088] As apparently from the above, according to the twenty eighth aspect of the present invention, it is possible to encrypt each of information units with different encryption system, ensuring the encryption resistance against unfair access the information.

[0089] According to a twenty ninth aspect, in the twenty eighth aspect of the present invention, an information transmission system further comprising:

a third encryption unit for encrypting the multiplexed information with a third predetermined encryption system to produce an encrypted multiple information unit.

[0090] According to a thirtieth aspect, in the twenty ninth aspect of the present invention, an information transmission system, wherein the third predetermined encryption system is the same as that applied to the encrypted information.

[0091] According to a thirty first aspect, in the twenty ninth aspect of the present invention, an information transmission system, wherein the second predetermined encryption system is the same as the third predetermined encryption system.

[0092] According to a thirty second aspect, in the twenty ninth aspect of the present invention, an information transmission system, wherein the first, second, and third predetermined encryption systems are the same.

[0093] According to a thirty third aspect, in the twenty seventh aspect of the present invention, an information transmission system further comprising:

a transmitter for converting the encrypted multiplexed information into a format suitable for an efficient transmission.

[0094] According to a thirty fourth aspect, in the twenty seventh aspect of the present invention, an information transmission system, wherein the first encryption unit encrypts the information unit with an encryption system suitable for the transmission of information.

[0095] According to a thirty fifth aspect, in the twenty seventh aspect of the present invention, an information transmission system further comprises:

a second demultiplexer for demultiplexing the second multiplexed information unit;
a third decryption unit for decrypting the second encrypted information unit with a third predetermined decryption system to produce the information unit.

[0096] According to a thirty sixth aspect, in the twenty seventh aspect of the present invention, an information transmission system, wherein the first decryption system is the same as that applied to the encrypted information.

[0097] According to a thirty seventh aspect, in the twenty seventh aspect of the present invention, an information transmission system apparatus further comprises:

a storage provided between the first demultiplexer and the second decryption unit for storing any of the first and second encrypted information units.

[0098] According to a thirty eighth aspect, in the thirty aspect of the present invention, an information transmission system further comprises:

a reproducer for receiving the encrypted information units from the second decryption unit to produce a reproduction information indicating a content the encrypted information, the reproducer requesting the storage to supply the stored encryption information unit to the second decryption unit.

BRIEF DESCRIPTION OF THE DRAWINGS

[0099]

Fig. 1 is a block diagram showing an information transmission apparatus according to a first embodiment of the present invention,
Fig. 2 is a graph in assistance of explaining an encrypted multiple information unit produced by the information transmission apparatus of Fig. 1,
Fig. 3 is a flow chart showing operations performed by the transmitting unit and transmitter in the information transmission apparatus of Fig. 1,
Fig. 4 is a flow chart showing operations performed by the receiving unit in the information transmission apparatus according of Fig. 1.
Fig. 5 is a block diagram showing an information transmission apparatus according to a second embodiment of the present invention,
Fig. 6 is a graph in assistance of explaining an encrypted multiple information unit produced by the information transmission apparatus of Fig. 5,
Fig. 7 is a flow chart showing operations performed by the transmitting unit and transmitter in the information transmission apparatus of Fig. 5,
Fig. 8 is a flow chart showing operations performed by a receiving unit in the information transmission apparatus of Fig. 5,
Fig. 9 is a block diagram showing an alternative of the information transmission apparatus of Fig. 5,
Fig. 10 is a block diagram showing an information transmission apparatus according to a third embodiment of the present invention,
Fig. 11 is a graph in assistance of explaining an encrypted multiple information unit produced by the information transmission apparatus of Fig. 10,
Fig. 12 is a flow chart showing operations performed by a receiving unit in the information transmission apparatus of Fig. 10,
Fig. 13 is a block diagram showing an alternative of the information transmission apparatus of Fig. 10,
Fig. 14 is a block diagram showing an information transmission apparatus according to a fourth embodiment of the present invention,
Fig. 15 is a flow chart showing operations performed by a transmitting unit and transmitter in the information transmission apparatus of Fig. 14,
Fig. 16 is a flow chart showing operations performed by a receiving unit in the information transmission apparatus of Fig. 14,
Fig. 17 is a flow chart showing operations performed by storage in the information transmission apparatus of Fig. 14,
Fig. 18 is a block diagram showing an information transmission apparatus according to a fifth embodiment of the present invention,
Fig. 19 is a flow chart showing operations performed by a transmitting unit and transmitter in the information transmission apparatus of Fig. 18,
Fig. 20 is a flow chart showing operations performed by a receiving unit in the information transmission apparatus of Fig. 18,
Fig. 21 is a block diagram showing an alternative of the information transmission apparatus of Fig. 18,
Fig. 22 is a block diagram showing an information transmission apparatus according to a sixth embodiment of the present invention,
Fig. 23 is a flow chart showing operations performed by a receiving unit in the information transmission apparatus of Fig. 22,
Fig. 24 is a block diagram showing an alternative of the information transmission apparatus of Fig. 22,
Fig. 25 is a block diagram showing a conventional information transmission apparatus,
Fig. 26 is a graph in assistance of an encrypted multiple information unit produced by the information transmission apparatus of Fig. 25,
Fig. 27 is a flow chart showing operations performed by the transmitting unit and transmitter in the information transmission apparatus of Fig. 25, and
Fig. 28 is a flow chart showing operations performed by a receiving unit in the information transmission apparatus of Fig. 25.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0100] Preferred embodiments according to the present invention are described in detail with reference to the attached drawings Figs. 1 to 24.

(First Embodiment)

[0101] With reference to Figs. 1 to 3, here below, an information transmission apparatus according to a first embodiment of the present invention is described. Description is now made by taking two types of specific examples, those are information transmission in the Internet as Example 1 and digital broadcasting as Example 2. The information transmission apparatus 100 includes a transmitting unit 110, transmitter 120, and a receiving unit 130.

Transmitting unit 110

[0102] The transmitting unit 110 includes information unit generator 111, an information unit scrambler 112, a multiplexer 113, a lower layer scrambler 114, and, a sender 115. The information unit generator 111 generates a plurality of information units Iu, and outputs thereof. In Example 1, the information unit generator 111 outputs the information units Iu which are, for example, a text the user entered with a keyboard or the like, and an image taken into a computer, and others already stored in the computer. The information unit generator 111 may be an input screen portion of electronic mail software, and a server in a broadcasting station on the Internet, for example.

[0103] On the other hand, in Example 2, all information units Iu generated are previously stored in the information unit generator 111. A method for merely selectively outputting the information units Iu in accordance with a predetermined schedule is considered. The information unit generator 111 is a broadcasting station system containing a program management system in a sending system of digital broadcasting, a cart machine of a VTR, an MPEG-2 encoder, an EPG (Electronic Program Guide) management sending system of digital broadcasting, and the like. Additional information such as EPG must be sent out with the same contents thereof maintained for a long time. Therefore, the same contents may, in some cases, are repeatedly outputted in a period on the order of seconds in the information unit generator 111.

[0104] The information unit scrambler 112 is connected to the information unit generator 111 for receiving the information unit Iu therefrom to encrypt the inputted information units Iu. Then the information unit scrambler 112 outputs the result of encryption as an encrypted information units Iue. An object to be encrypted once is a set having elements which are information units Iu or the results of the encryption. The encrypted information unit Iue shall be defined as follows.

> Definition 1: The encrypted information unit Iue is also an information unit Iu.
>
> Definition 2: A set of information units Iu or encrypted information units Iu is also an encrypted information unit Iue.
>
> Definition 3: The result of encrypting an encrypted information unit Iue is also an encrypted information unit Iue.

[0105] The multiplexer 113 is connected to the information unit generator 111 and the information unit scrambler 112 for receiving the information unit Iu and the encrypted information unit, respectively, therefrom. Then, the multiplexer 113 multiplexes the information received from the information unit generator 111 and/or the information unit scrambler 112, and outputs the multiplexed result as a multiple information unit Im therefrom.

[0106] The multiplexer 113 is further connected to the output port thereof for receiving the multiple information Im produced thereby to multiplex again. Furthermore, the output port of the multiplexer 113 is also connected to the input port of the information unit scrambler 112, so that the information unit scrambler 112 can encrypts the multiple information unit Im to produce the encrypted information unit Iue.

[0107] Thus, the multiplexer 113 handles the encrypted information units Iue outputted by the information unit scrambler 112 as objects to be multiplexed, similarly to the information units Iu outputted by the information unit generator 111. The encrypted information units Iue handed at a time by the information unit scrambler 112 are handled upon being considered to be equal to one information unit Iu. The multiplexer 113 may add the information units Iu outputted from the information unit generator 111 to the encrypted information units Iue previously inputted from the information unit scrambler 112, and multiplex them.

[0108] Specifically, the multiplexer 113 receives the plurality of information units Iu outputted by the information unit generator 111. Then, the multiplexer 113 multiplexes the inputted information units Iu, and outputs the multiplexed information units Iue as multiple information Im. By the multiplexing, the plurality of information units Iu are converted into a format (multiple information Im) suitable for efficient transmission in the transmitter 120.

[0109] In Example 1, the multiplexer 113 is an MIME (Multi-purpose Internet Mail Extensions) encoder used for sending multimedia information by an electronic mail on the Internet, for example. In this case, the multiplexer 113 respectively takes text information, image information, voice information, and so forth which are the plurality of information units Iu as parts. Then the multiplexer 113 converts the parts into a multipartite message conforming to MIME for collecting the plurality of parts, and outputs the message. The formal specification of the MIME is defined by RFC (Request for Comments) 1521/1522.

[0110] On the other hand, in Example 2, the multiplexer 113 is a service multiplexer for obtaining TS (Transport Stream) of an MPEG-2 systems from a plurality of stream data, for example. The MPEG-2 systems and the TS are standardized by ISO/IEC CD 13818-1. In this case, the multiplexer 113 divides each of the plurality of information units Iu outputted by the information unit generator 111 into packets called PES (Packetized Elementary Stream), and multiplexes the obtained packets on the basis of a predetermined rule.

[0111] The lower layer scrambler 114 is connected to the multiplexer 113 for receiving the multiple information Im therefrom to encrypt thereof. Then, the lower layer scrambler 114 outputs the encryption result as the encrypted multiple information Ime therefrom. Specifically, the lower layer scrambler 114 receives the multiple information Im outputted by the multiplexer 113, and encrypts the multiple information Im in accordance with a predetermined encryption algorithm. Then, the lower layer scrambler 114 outputs the encrypted result as encrypted multiple information Ime.

[0112] In Example 1, the lower layer scrambler 114 may be software PGP (Pretty Good Privacy) on which an RSA cipher which is a public key cipher, for example, mounted therein is started with an encryption option. An output of the lower layer scrambler 114 is a text of an electronic mail encrypted using the RSA cipher. The RSA cipher is described in detail in an article entitled by R. L. Rivest, A. Shamir, and L. Adleman which are contrivers themselves "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" (Vol. 21, No. 2 issued on February, 1978 in Communications of the ACM). The PGP is described in detail in an article entitled by Simson Garfinkel "PGP: Pretty Good Privacy" (O'Reilly & Associates).

[0113] On the other hand, in Example 2, the lower layer scrambler 114 may be, for example, a scrambler of a transport layer. The lower layer scrambler 114 encrypts a payload portion of inputted TS of MPEG-2 using an encryption algorithm such as MULTI2, and outputs the encrypted TS of the MPEG-2 which is the result thereof.

[0114] The sender 115 is connected to the lower layer scrambler 114 for receiving the encrypted multiple information Ime therefrom to produce the transmission information It, and outputs produced transmission information It therefrom. Specifically, the sender 115 converts the encrypted multiple information Ime outputted from the lower layer scrambler 114 into the transmission information It which will be inputted to the transmitter 120.

[0115] In Example 1, the sender 115 is a program for adding a mail header composed of a destination field, a sender field, and so forth to the text of the electronic mail. An output of the sender 115 is the text of the electronic mail to which the mail header is added. On the other hand, in Example 2, the sender 115 is an error-correcting encoder and a modulator for the TS of the MPEG-2.

Transmitter 120

[0116] The transmitter 120 receives the transmission information It outputted by the sender 115, and transmits the transmission information It to a physically distant point. Both inputs and outputs of the transmitter 120 are the transmission information It. All the inputs of the transmitter 120 may not appear in the outputs to the receiving unit 130 without any error. In Example 1, the transmitter 120 is a plurality of mail communication daemons which are connected to each other by a channel such as the Internet for interpreting and executing an SMTP (Simple Mail Transfer Protocol). Examples of the typical mail communication daemon include "sendmail". The formal specification of the SMTP is defined by RFC 821, RFC 822, and RFC 974. The sendmail is described in detail in an article entitled by E. Allman ""SENDMAIL - An Internetwork Mail Router" Unix Programmer's manual" (CSRG U. C. Berkeley issued on July, 1983).

[0117] On the other hand, in Example 2, the transmitter 120 is constituted by an up-converter, a parabola antenna for sending data to a satellite, a communication satellite, and a ground receiving antenna.

Receiving unit 130

[0118] The receiving unit 130 receives the transmission information It from the transmitter 120. Then, the receiving unit 130 variously processes the transmission It to reproduce the information unit Iu included therein, and finally presents the reproduction information Ir which is the contents of information unit Iu to a user. The receiving unit 130 includes receiver 131, a lower layer descrambler 132, demultiplexer 133, an information unit descrambler 134, reproducer 135, and presenter 136.

[0119] The receiver 131 is connected to the transmitter 120 for receiving the transmission information It therefrom, and produces the encrypted multiple information Ime. Specifically, the receiver 131 receives the transmission information It outputted by the transmitter 120, and takes out the whole or a part of thereof, then, the receiver 131 produces the encrypted multiple information Ime based on the transmission information It.

[0120] In Example 1, the receiver 131 is a front end program for mail transmission. On the other hand, in Example 2, the receiver 131 is the connection of a satellite broadcasting tuner, a demodulator and an error-correcting decoder.

[0121] The lower layer descrambler 132 is connected to the receiver 131 for receiving the encrypted multiple information Ime therefrom, and produces the multiple information Im. The lower layer descrambler 132 receives the encrypted multiple information Ime outputted by the receiver 131, and decrypts the encrypted multiple information Ime, and produces the multiple information Im. In Example 1, the lower layer descrambler 132 is a PGP program which is started with a decryption option. On the other hand, in Example 2, the lower layer descrambler 132 is a descrambler of the transport layer.

[0122] Note that, the encrypted multiple information Ime produced by the lower layer descrambler 132 is substantially the same in content as the encrypted multiple information Ime produced by the lower layer scrambler 114 of the transmitting unit 110, but can be different in the encrypting format or encrypting method. Of course, it is also possible to reproduce the completely same encrypted multiple information Ime as that produced by the lower layer scrambler 114.

[0123] The demultiplexer 133 is connected to the lower layer descrambler 132 for receiving the multiple information Im therefrom. The demultiplexer 133 separates the encrypted information unit Iue from the multiple information Im, and outputs the separated encrypted information unit Iue therefrom. When the information decrypted from the multiple information includes the information unit Iu which does not need the decryption, the demultiplexer 133 outputs the encrypted information unit Iue and the information unit Iu, separately.

[0124] Specifically, in Example 1, the demultiplexer 133 is an MIME decoder, and separates the text information, the image information, and so forth which are the respective parts included in the multipartite message as separate information, to take out the separate information. On the other hand, in Example 2, the demultiplexer 133 is a demultiplexer for the TS of the MPEG-2. The demultiplexer 133 separates a plurality of streams which are multiplexed by the MPEG-2 systems.

[0125] The information unit descrambler 134 is connected to the demultiplexer 133 for receiving only the encrypted information unit Iue therefrom. Then, the information unit descrambler 134 decrypts the received encrypted information unit Iue to produce the information unit Iu. However, when the encrypted information unit Iue is a multiple encrypted information unit such as those repeatedly encrypted by the information unit scrambler 112, or repeatedly multiplexed by the multiplexer 113, as described in the above.

[0126] In the former case that the encrypted information unit Im has been repeatedly encrypted by the scrambler 112, another encrypted information unit Iue still remains even after decryption by the information unit descrambler 134 itself. The information unit descrambler 134 outputs such remained encrypted information unit Iue and information unit Iu separately from discrete output ports, respectively. For decrypting such remained encrypted information unit Iue, the information unit descrambler 134 is further connected to one of output ports thereof for returning the remained encrypted information unit Iue thereto. The information unit descrambler 134 repeats this feed back operation, until the remained encrypted information unit Iue does not appear after decryption thereby.

[0127] In the latter case that the encrypted information unit Iue has been repeatedly multiplexed by the multiplexer 113, another multiple information unit Im still remains therein even after demultiplexing by the demultiplexer 133. Since such remained multiple information unit is hierarchically multiplexed and encrypted, it is necessary first to decrypt the outer shell of remained encrypted (repeatedly multiplexed) information unit Iue before decryption by the information unit descrambler 134 itself. Therefore, such remained multiplexed encrypted (repeatedly multiplexed) information Iue is returned to the demultiplexer 133. Resultantly, repeated demultiplexing by the demultiplexer 133 and/or decryption by descrambler 134 continues till no multiple information unit Im but decrypted information unit Iu remains after decryption. Then, the information unit descrambler 134 outputs only the information unit 1 therefrom.

[0128] Specifically, the information unit descrambler 134 receives the encrypted information unit Iue outputted by the information unit descrambler 134. Then, the information unit descrambler 134 outputs an encrypted information unit Iue or an information unit Iu which is the result of decrypting the encrypted information unit Iue outputted therefrom. The encrypted information unit Iue is obtained by subjecting the information unit Iu to encryption a plurality of times. Therefore, the encrypted information unit Iue must be decrypted a plurality of times in order to take out the information unit Iu.

[0129] The information unit descrambler 134 receives the output of the information unit descrambler 134 itself again, and repeatedly decrypts the input, thereby making it possible to decrypt the encrypted information unit Iue obtained by performing encryption a plurality of times. Even if the number of times of decryption which can be performed at a time by the information unit descrambler 134 is one, therefore, an information unit Iu can be finally taken out of the encrypted information unit Iue. The information unit descrambler 134 may be able to simultaneously perform a plurality of times of decryption. In the case, the information unit Iu can be taken out at higher speed.

[0130] The reproducer 135 is connected to the information unit descrambler 134 and to the other of input ports of the demultiplexer 133 for receiving the information unit Iu therefrom. Then, the reproducer 135 converts the inputted information unit Iu into reproduction information Ir which is reproducible information, and outputs the reproduction information Ir therefrom. In Example 1, the reproducer 135 may be a text file viewer, image file presenting software, etc. On the other hand, in Example 2, the reproducer 135 may be an MPEG-2 decoder for reproducing voices or images encoded by the MPEG-2, for example. In this case, the output is an NTSC (National Television System Standard Committee) signal or an analog voice signal.

[0131] The presenter 136 receives the reproduction information outputted by the reproducer 135, and presents an information unit Iu to a user. Specifically, the presenter 136 receives the reproduction information

Ir outputted by the reproducer 135, and presents the information contained in the reproduction information Ir to a user. In Example 1, the presenter 136 may be a window system such as X-window or Microsoft Windows for presenting image and voice to a user. On the other hand, in Example 2, the presenter 136 may be a television receiver for inputting and receiving an NTSC signal and an analog voice signal, for example.

In Operation

[0132] With reference to Figs. 3 and 4, general operations performed by the information transmission apparatus 100 will be described bellow. In Fig. 3, the operations performed by the transmitting unit 110 and the transmitter 120 are shown.

[0133] At step S301, the information unit generator 111 generates a plurality of information units Iu, and outputs the generated information units Iu therefrom. Examples of the generation of the information units Iu include a method in which a user enters information units Iu and designates a file as in Example 1. The information units Iu are selectively outputted from stored information units Iu in accordance with a predetermined schedule as in Example 2.

[0134] At step S302, information unit scrambler 112 recursively encrypts the information units Iu generated at step S301, and produces the results thereof as encrypted information units Iue.

[0135] At step S303, the plurality of encrypted information units Iue produced by the encryption at step S302 are multiplexed, and outputs the result thereof as multiple information Im. The ultiplexer 113 multiplexes the information units Iu generated at step S301, and outputs the result thereof as multiple information Im. The multiple information Im is multipartite data conforming to the MIME in the case of Example 1, while being data representing the TS of the MPEG-2 systems in the case of Example 2.

[0136] At step S304, the lower layer scrambler 114 encrypts the multiple information Im obtained by the multiplexing at step S303, and produces the encrypted multiple information Ime. In Example 1, the multiple information Im is encrypted using the RSA cipher or the like. On the other hand, in Example 2, the payload portion of the TS of the MPEG-2 is encrypted using a MULTI2 cipher manufactured by Hitachi Ltd. for example.

[0137] At step S305, the sender 115 converts the encrypted multiple information Ime obtained by the encryption at step S304 into a format which is suitable for transmission by the transmitter 120, and produces the transmission information It. In Example 1, information obtained by adding information, for example, "To:" field, "From:" to the head of the text of the mail which is encrypted multiple information Ime is outputted as the transmission information It. On the other hand, in Example 2, the information obtained by encoding the TS of the MPEG-2 using an error-correcting code and then, modulating the encoded TS is outputted.

[0138] At step S306, the transmitter 120 transmits the transmission information It to a physically distant point. A plurality of receiving units 130 may correspond to one transmitting portion. In Example 1, the mail communication daemons mounted on one or a plurality of computers connected are communicated to a computer network such as the Internet or a LAN (Local Area Network) on the basis of the SMTP. Thus, the mail is transmitted from the mail communication daemon ogn one of the computers to the mail communication daemon on the other computer.

[0139] On the other hand, in Example 2, transmission information It obtained by the conversion in the up-converter is transmitted to the communication satellite by the parabolic antenna. The communication satellite transmits the received transmission information It to the ground by a transponder. The transmission information It from the communication satellite is received by the ground receiving antenna.

[0140] In Fig. 4, the operations performed by the receiving unit 130 are shown. At step S401, the receiver 131 receives the transmission information It outputted from the transmitter 120, and takes out a part or the whole of encrypted multiple information Ime from the received transmission information It. In Example 1, processing for taking out one electronic mail data addressed to a specific user is performed. On the other hand, in Example 2, processing for filtering a particular packet storing information to be found by a PID (Packet ID), and selecting and extracting the packet is performed by tuning to a predetermined frequency.

[0141] At step S402, the lower layer descrambler 132 receives the encrypted multiple information Ime generated at step S401, and decrypts the received encrypted multiple information Ime. Then, the lower layer descrambler 132 outputs the decryption result as the multiple information Im. In Example 1, the lower layer descrambler 132 is the PGP program started with a decryption option. Decryption is performed using the RSA cipher by the PGP program, and the result of the decryption is outputted. On the other hand, in Example 2, the multiple information Im encrypted using the MULTI2 cipher is decrypted, to obtain multiple information Im.

[0142] At step S403, the demultiplexer 133 separates the encrypted information unit Iue from the multiple information unit Im obtained at step S402. In Example 1, the demultiplexer 133 separates for each part of the multipartite message obtained by multiplexing on the basis of the MIME. As a result, the text information, the image information, the voice information, and so forth which are the respective parts are separated as discrete information units Iu.

[0143] On the other hand, in Example 2, the demultiplexer 133 separates the plurality of streams multiplexed by the MPEG-2 systems on the basis of a PID

(Packet ID, a packet identifier). As a result, additional information such as an MPEG-2 video stream, an MPEG-1 audio stream, and EPG are separated as discrete information units Iu. An MPEG-2 video is standardized by ITU-T H. 262, and an MPEG-1 audio is standardized as ISO/IEC 11172-3 Standard.

[0144] At step S404, it is judged whether the information after being demultiplexed by the demultiplexer 133 includes an encrypted information unit Iue or not. When it is judged YES, meaning that that information produced by the demultiplexer 133 at step S403 needs decryption to take out the content therefrom, the procedure advances to step S405.

[0145] At step S405, the information unit descrambler 134 decrypts once the encrypted information unit Iue outputted from the demultiplexer 133. Thereafter, the procedure returns to step S403. By repeatedly carrying out the operation at steps S403, S404, and S405, the information unit descrambler 134 can decrypt all the encrypted information unit Iue included in the multiple information Im, and finally take out all the information unit Iu sent from the transmitting unit 110.

[0146] On the other hand, when it is judged NO at step S404, meaning that that information after being demultiplexed by the demultiplexer 133 does not need decryption to take out the content therefrom. In other words, the information outputted from the demultiplexer 133 is information unit Iu only. Then, the procedure advances to step S406.

[0147] At step S406, the reproducer 135 receives the information unit Iu outputted by the descrambler 134, and produces reproduction information Ir which is reproducible information. In Example 1, when the information unit Iu is text information, for example, fonts corresponding to respective character codes are selected and listed, to produce a bitmap format as the reproduction information Ir. When the information unit Iu is in an image information format such as JPEG (Joint Photographics Experts Group), it is expanded into the bitmap format, and the result of the expansion is outputted as reproduction information. The JPEG is standardized by ISO/IEC 10918. When the information unit Iu is voice information, it is converted into an analog voice signal by the same function as that of a digital-to-analogue (D/A) converter. And the analog voice signal is also outputted as reproduction information.

[0148] On the other hand, in Example 2, when the information unit Iu obtained at step S301 is the MPEG-2 video stream, the MPEG-2 video is decoded, and outputs the NTSC signal as reproduction information. When the information unit Iu is a voice stream, it is converted into an analog voice signal by D/A conversion, and the analog voice signal is outputted.

[0149] At step S407, the presenter 136 receives the reproduction information Ir outputted from the reproducer 135, and then presents the contents of reproduction information Ir to a user in accordance with the format of the reproduction information. In Example 1, when the reproduction information obtained at step S406 is in the bitmap format, the presenter 136 arranges and presents the reproduction information Ir on a display screen. Thus, the reproduction information Ir is presented to the user. When the reproduction information obtained at step S406 is an analog voice signal, the analog voice signal is converted into sound by being sent to a speaker, and is visually presented to the user.

[0150] On the other hand, in Example 2, an NTSC signal as the reproduction information which is obtained at step S406 is received on a display, the analog voice information is sent to a speaker, and the reproduction information is presented to the user.

[0151] As described in the foregoing, in the first embodiment, it is possible to handle the information unit Iu which has been recursively encrypted a plurality of times. Therefore, it is possible to introduce a hierarchical structure into the encryption of the information unit Iu. The correspondence of the hierarchical structure to the structure of a program makes it possible to encrypt, in cases such as a case where a part of a set of information units Iu is selectively purchased, the information unit Iu only by performing one type of encryption a smaller number of times.

[0152] The information unit descrambler 134 repeatedly performs decryption in the receiving unit 130, to take out the information unit Iu. Therefore, the receiving unit can be constructed without requiring such a high-level or special descrambler as to correspond to a plurality of types of ciphers and perform a plurality of times of decryption processing at a time, thereby making it possible to realize simplification and cost reduction.

Encoding information units into encrypted multiple information unit

[0153] With reference to Fig. 2, the encrypted multiple information unit Ime produced by the information transmission apparatus 100 is described. Various processing levels of information units are expressed with different suffixes for the sake of better recognition thereof. For example, the output from the lower layer scrambler 114, represented by a rectangle of a dot line, is the encrypted multiple information Ime0a.

[0154] The four outputs from the information unit generator 111, indicated by circles, are the information units Iu1a, Iu2a, Iu3a, and Iu4a, respectively. These information units Iu1a, Iu2a, Iu3a, and Iu4a represent, for example, a tourist resort guide considering the weather forecast, a weather forecast for the tourist resort, a weather forecast for allover the country, and a weather forecast for a local area, respectively.

[0155] The rectangles Iue1a, Iue12a, and Iue4a each indicated by a solid line represent the units of encrypted information produced inside the transmitting unit 110 of the information transmission apparatus 100 at respective encryption stages. Specifically, the rectangle Iue1a represents a first encrypted information unit Iue which is produced, such that the information unit scrambler 112 encrypts the information unit Iu1a outputted from the information unit generator 111 with a first predetermined cipher C1 under a first predetermined encryption system CS1 at step S302. Thus, the first encrypted information unit Iue1a is produced.

[0156] The rectangle Iue12a represents also a second encrypted information unit Iue which is produced at the following two steps. At step S303, the multiplexer 113 multiplexes the first encrypted information unit Iue1a received from the information unit scrambler 112 and the information unit Iu2a, and produces a multiple information unit Im12a (not shown). At step S302, the information unit scrambler 112 encrypts the multiple information unit Im12a received from the multiplexer 113 with a second predetermined cipher C2 under a second predetermined encryption system CS2 at step S302. Thus, the second encrypted information unit Iue12a wherein the information unit Iu1a is encrypted twice is produced.

[0157] The rectangle Iue4a represents a third encrypted information unit Iue which is produced, such that the information unit scrambler 112 encrypts the information unit Iu4a outputted from the information unit generator 111 with a third predetermined cipher C3 under a third encryption system CS3 at step S302. Thus, the third encrypted information Iue4a is produced.

[0158] The rectangle Ime0a represents an encrypted multiple information Ime which is produced as follows. First, the multiplexer 113 multiplexes the second encrypted information unit Iue12a, the information unit 3a, and third encrypted information unit Iue4a, and produces a multiple information unit Im1234a (not shown) at step S303. Second, the lower layer scrambler 114 encrypts the multiple information unit Im1234 with a fourth predetermined cipher C4 under a fourth predetermined encryption system CS4 at step S304.

[0159] As a result, the first information unit Iu1a is encrypted thrice with the first, second, and fourth predetermined ciphers C1, C2, and C4. The second information unit Iu2a is encrypted twice with the second and fourth predetermined ciphers C2, and C4. The third information unit Iu3a is encrypted once with the fourth predetermined cipher C4. The fourth information unit Iu4a is encrypted twice with the third and fourth predetermined ciphers C3 and C4.

[0160] Thus, there is a hierarchical order among these information unit Iu1a, Iu2a, Iu3a, and Iu4a representing different contents of weather forecast program. Specifically, the encrypted multiple information Ime0a is a set of information having meanings for a user. The set is one electronic mail or one information program, for example. The encrypted multiple information unit Ime0a recursively includes a portion (Iu3a) which is not encrypted and a portion (Iue12a and Iue4a) which is encrypted therein.

[0161] Note that each of all ciphers C1, C2, C3, and C4 can be assigned with the same value or any optional value according to the suitable resistance of cipher necessary to protect the information unit against unfair access thereto. Similarly, each of all encryption system CS1, CS2, CS3, and CS4 can be selected from the identical encryption system or various different encryption system such as examples referred in the above.

[0162] Considered as an example in which non-encrypted portion (Iu3a) and encrypted portion (Iue12a and Iue4a) are included in one encrypted multiple information unit (Ime0a). The whole of an encrypted multiple information unit Ime0a is a weather forecast program, the non-encrypted portion (Iu3a) is a free weather forecast for allover the country, the encrypted portion (Iue12a and Iue4a) is a charged detailed forecast for the local areas. Furthermore, a preview of a film and the encrypted film, an article for introducing software, an execute form of encrypted software, and so forth are also considered.

[0163] In this case, the user can view the weather forecast for allover the country (Iu3a) by decrypting the encrypted multiple information unit Ime0a, the weather forecast for the tourist resort (Iu2a) by decrypting the encrypted information unit Iue2a, the tourist resort guide considering the weather forecast (Iu1a) by decrypting the encrypted information unit Iue1a, and the weather forecast for a local area (Iu4a) by decrypting the encrypted information unit Iue4a, respectively.

[0164] Thus, the information unit encrypted plural times with discrete ciphers has the same resistance against an unfair decryption as in the case that it is decrypted with a single cipher having a resistance corresponding to those plural discrete ciphers. Furthermore, plural information units, such as information units Iue1a and Iu2a according to definition 2 are encrypted at the same time in the same encryption level, enabling to reducing a burden to starting the decrypting operation.

<u>Decoding encrypted multiple information unit into information unit</u>

[0165] The encrypted information encrypted with ciphers in hierarchically arranged by the transmitting unit 110 can be decrypted by repeatedly using a single of descrambler with a simply constructed apparatus, which will be specifically described below. The encrypted multiple information unit Ime0a is supplied to the receiving unit 130 through the transmitter 120 in the format of transmission information It.

[0166] The receiver 131 of the receiving unit 130 takes out a part or the whole of encrypted multiple information Ime0a from the received transmission information It at step S401. At step S402, the lower layer descrambler 132 decrypts the received encrypted multiple information Ime0a with the fourth predetermined cipher C4 to obtain the multiple information unit Im1234a (not shown) constructed by the second encrypted information unit Iue12a, the third information unit Iu3a, and the third encrypted information unit Iue4a. Note that thus obtained multiple information unit Im1234a can be produced in a format different from that of the multiple information unit Im1234a produced by the multiplexer 113 at Step S303.

[0167] The demultiplexer 133 demultiplexes the multiple information unit Im1234a produced at step S402, and separates each of encrypted information unit Iue and/or information unit Iu therefrom at step S403. Thus, the second encrypted information unit Iue12a, the third information unit Iu3a, and the third encrypted information unit Iue4a are produced at step S403. Note that thus obtained information units Iue12a, Iu3a, and Iue4a can be produced in the formats different from those produced by the information unit scrambler 112 of the transmitting unit 110. Needless to say that those information units Iue12a, Iu3a, and Iue4a can be in the same formats as those produced by the information unit scrambler 112 of the transmitting unit 110, resulting in the reproduction of those information units Iue12a, Iu3a, and Iue4a.

[0168] The second encrypted information unit Iue12a is sent to the information unit descrambler 134 where the multiple information unit Im12a (not shown) is produced by decrypting the encrypted information unit Iue12a with the second predetermined cipher C2 at step S405. Thus produced multiple information unit Im12a is sent back to the demultiplexer 133 where the first encrypted information unit Iue1a and the second information unit Iu2a are produced by demultiplexing the multiple information unit Im12a at step S403.

[0169] At step S404, the first encrypted information unit Iue1a is sent to the information unit descrambler 134, where the first information unit Iu1a is produced by decrypting the encrypted information unit Iue1a with the first predetermined cipher C1. Similarly, the third encrypted information unit Iue4a is sent to the information unit descrambler 134, where the fourth information unit Iu4a is produced.

[0170] Each of information units Iu1a produced at step S405, Iu2a produced at step S403, Iu3a produced at step S403, and Iu4a produced at step S405 are sent to the reproducer 135, where the reproduction information Ir are produced from those information units Iu1a, Iu2a, Iu3a, and Iu4a at step S406. Note that all information units Iu1a, Iu2a, Iu3a, and Iu4a can be produced in the substantially same in content as those produced by the information unit generator 111, but can be different in the encrypting format or encrypting method. Of course, it is also possible to reproduce the completely same information units as those Iu1a, Iu2a, Iu3a, and Iu4a produced by the information unit generator 111.

(Second Embodiment)

[0171] With reference to Figs. 5 to 8, here below, an information transmission apparatus according to a second embodiment of the present invention is described. The information transmission apparatus 500 includes a transmitting unit 510, transmitter 120, and a receiving unit 530. The transmitter 120 is the same as that used in the information transmission apparatus 100. Here below, descriptions of any of substantially the same components constructing the information transmission apparatus 100 are generally omitted for reducing the redundancy.

[0172] Note that the encrypted multiple information Ime produced by a descrambler 532 is substantially the same in content as the encrypted multiple information Ime produced by the lower layer scrambler 114 of the transmitting unit 110, but can be different in the encrypting format or encryption method. Of course, it is also possible to reproduce the completely same encrypted multiple information Ime as that produced by the lower layer scrambler 114.

Transmitting unit 510

[0173] The transmitting unit 510 has a construction very similar to that of the transmitting unit 110 shown in Fig. 1, such that the information unit scrambler 112 is replaced by an information unit scrambler 512. Compared with the information unit scrambler 112, the information unit scrambler 512 should be able to encrypt the information unit Iu conforming to a lower layer transmission performed by a transmitter 120. In other words, the information unit scrambler 512 only have to encrypt under a certain encryption system used by a lower layer such as being performed by the transmitter 120. Needless to say, the information unit scrambler 512 may be able to encrypt under various encryption systems including one suitable for the above mentioned lower layer transmission.

[0174] Specifically, as the cipher used in the information unit scrambler 512, a cipher which can be decoded by sharing a device having high tamper resistance used for decryption performed in the scrambler 514 may be selected. The device having high tamper resistance is a device which is subjected to such measures that stored contents are erased if they are unfairly decomposed, and information relating to secrecy is not let out from an LSI (Large Scale Integrated Circuit) where it is difficult to analyze without special facilities. For example, an IC card used for a receiver for CS digital broadcasting is a device having high tamper resistance.

Receiving unit 530

[0175] The receiving unit 530 has a construction similar to that of the receiving unit 130 shown in Fig. 1, such that the lower layer descrambler 132 and the information unit descrambler 134 are replaced by a descrambler 532 and a demultiplexer 533. The descrambler 532 is connected to the receiver 131 for receiving the encrypted multiple information unit Ime therefrom.

Then, the descrambler 532 decrypts the received multiple information unit Ime once, and produces the multiple information Im. Note that the descrambler 532 can decrypt any encrypted multiple information unit which is encrypted under various encryption systems including a certain encryption system adopted by the lower layer scrambler 114 in the transmitting unit 110.

[0176] The demultiplexer 533 is connected to the descrambler 532 for receiving the multiple information Im therefrom, and demultiplexes the received multiple information Im to produce the information unit Iu. However, when the multiple information Im produced by the descrambler 532 includes the repeatedly multiplexed information unit therein, the encrypted information unit Iue remains after demultiplexing.

[0177] The descrambler 532 is further connected to the demultiplexer 533 for receiving that remained encrypted unit Iue therefrom. Then, the descrambler 532 decrypts the encrypted unit Iue, and produces the multiple information unit Im, which will be supplied to the demultiplexer 533. When the encrypted information unit Iue received from the demultiplexer 533 is simply encrypted but not multiplexed, produced therefrom is an information unit Iu which will be directly supplied to the reproducer 135. Thus, the demultiplexer 533 is not required to be able to demultiplex the repeatedly mutiplexed information unit Im, but only have to be able to demultiplex an information unit Im which is multiplexed once.

[0178] Thus, the construction in the second embodiment is obtained by removing such a restriction that recursive encryption is performed a plurality of times by the information unit scrambler 112 from the construction in the first embodiment. The lower layer descrambler 132 and the information unit descrambler 134 which perform decryption in the first embodiment are integrated into the descrambler 532 this embodiment. The integration can be also considered to be the realization of the function of the information unit descrambler 134 by the function of the lower layer descrambler 132.

In Operation

[0179] With reference to Figs. 7 and 8, general operations performed by the information transmission apparatus 500 will be described bellow. The operations performed by the transmitting unit 510 and the transmitter 120 shown in Fig. 7 are very similar to those that are already described with reference to Fig. 3. Therefore, the operations are briefly described to clarify the distinction between them.

[0180] At step S601, the information unit generator 111 generates a plurality of information units Iu, and outputs the generated information units Iu therefrom.

[0181] At step S602, the information unit scrambler 512 encrypts the information units Iu generated at step S601 once, and outputs the results thereof as encrypted information units Iue. Specifically, the information unit scrambler 512 encrypts the information unit Iu conforming to a lower layer transmission performed by a transmitter 120. Specifically, a cipher used herein is of the same type as that of a cipher used in the lower layer scrambler 114. The "same" means that when the lower layer scrambler 114 uses an RSA cipher, for example, the information unit scrambler also performs encryption using the RSA cipher. Processing for recursively encrypting the information unit Iu a plurality of times is performed at step S302 in the first embodiment, while such a restriction that the information unit Iu is encrypted a plurality of times is not placed at this step.

[0182] At step S603, the multiplexer 113 multiplexes the plurality of encrypted information units Iue produced by the encryption at step S602, and outputs the result thereof as multiple information Im therefrom.

[0183] At step S604, the lower layer scrambler 114 encrypts the multiple information m obtained by the multiplexing at step S603 with the same cipher used at step S602. A cipher used in the lower layer scrambler 114 is the same as the cipher used in the information unit scrambler 112, as in the description of the information unit scrambler 512.

[0184] At step S605, the sender 115 converts the encrypted multiple information Ime obtained by the encryption at step S604 into a format which is suitable for transmission by the transmitter 120, and produces the transmission information It.

[0185] At step S606, the transmitter 120 transmits the transmission information It to a physically distant point.

[0186] In Fig. 8, the operations performed by the receiving unit 530 are similar to those that are already described with reference to Fig. 4. Therefore, the operations are briefly described to clarify the distinction between them. At step S701, the receiver 131 receives the transmission information It outputted from the transmitter 120, and takes out a part or the whole of encrypted multiple information Ime from the received transmission information It.

[0187] At step S702, the descrambler 532 receives the encrypted multiple information Ime generated at step S701, and decrypts the received encrypted multiple information Ime. Then, the descrambler 532 outputs the decryption result as the multiple information Im.

[0188] At step S703, the demultiplexer 533 separates the encrypted information unit Iue from the multiple information unit Im obtained at step S702. The demultiplexer 533 demultiplexes the repeatedly mutiplexed information unit Im, but demultiplexes an information unit Im which is multiplexed once.

[0189] At step S704, the descrambler 532 decrypts the encrypted multiple information unit Ime from the receiver 131 and/or the encrypted information unit Iue from the demultiplexer 533. From the encrypted information unit Ime or encrypted information unit Iue which is encrypted once, produced is the information unit Iu which will be directly supplied to the reproducer 135. From the encrypted information unit Ime or encrypted information unit Iue which is encrypted and multiplexed, produced is the multiple information unit Im which is supplied to the demultiplexer 533.

[0190] Specifically, when the information unit Iu is encrypted once, the encrypted information unit Iue is decrypted once, thereby making it possible to generate an information unit Iu. Although there is such a restriction that the information unit Iu is recursively encrypted a plurality of times in the first embodiment, the restriction is not placed in the second invention.

[0191] At step S705, the reproducer 135 receives the information unit Iu outputted from the descrambler 532 and the demultiplexer 533, and produces reproduction information Ir which is reproducible information.

[0192] At step S706, the presenter 136 receives the reproduction information Ir outputted from the reproducer 135.

[0193] As described in the foregoing, the encryption performed by the information unit scrambler 512 is the same as the encryption performed by the lower layer scrambler 114. Thus, it possible for the single descrambler 532 to decode a cipher used in not only the lower layer scrambler 114 but also the information unit scrambler 512. That is, it is possible to decrypt the information unit Iu by preparing only one descrambler which is not special.

Encoding information units into encrypted multiple information unit

[0194] With reference to Fig. 6 similar to Fig. 2, the encrypted multiple information unit Ime produced by the information transmission apparatus 500 is described. The output from the lower layer scrambler 114, represented by a rectangle of a dot line, is the encrypted multiple information Ime0b.

[0195] The four outputs from the information unit generator 111, indicated by circles, are the information units Iu1b, Iu2b, Iu3b, and Iu4b, respectively. These information units Iu1b, Iu2b, Iu3b and Iu4b represent, for example, a tourist resort guide considering the weather forecast, a weather forecast for the tourist resort, a weather forecast for allover the country, and a weather forecast for a local area, respectively.

[0196] The rectangles Iue12b, and Iue4b each indicated by a dot line represent the units of encrypted information produced inside the transmitting unit 510 respective encryption stages. The rectangle Iue12b is produced, such that the multiplexer 113 multiplexes the information units Iu1b and Iu2b received from the information unit generator 111, and produces a multiple information unit Im12b (not shown) at step S603. Then, the information unit scrambler 512 once encrypts the multiple information unit Im12b received from the multiplexer 113 with a fifth predetermined cipher C5 under a fifth predetermined encryption system CS5, and then produces the encrypted information unit Iue12b at step S602.

[0197] The rectangle Iue4b represents also an encrypted information unit Iue which is produced, such that the information unit scrambler 512 encrypts the information unit Iu4b with a sixth predetermined cipher C6 under a sixth predetermined encryption system CS6 at step S602.

[0198] The encrypted multiple information unit Ime0b is produced, such that the multiplexer 113 multiplexes the encrypted information unit Iue12b, the information unit Iu3b, and the encrypted information unit Iue4b, and then produces a multiple information unit Im1234b (not shown) at step S603. Then, the lower layer scrambler 114 encrypts the multiple information unit Im1234b with a seventh predetermined cipher C7 under a seventh predetermined encryption system CS7 at step S604.

[0199] As a result, the information units Iu1b and Iu2b are both encrypted twice with the fifth, and seventh predetermined ciphers C5 and C7. The information unit Iu3a is encrypted once with the seventh predetermined ciphers C7. The information unit Iu4b is encrypted twice with the sixth and seventh predetermined ciphers C6 and C7.

[0200] Thus, there is a hierarchical order among these information unit Iu1b, Iu2b, Iu3b, and Iu4b representing different contents of weather forecast program. The hierarchical order according to this embodiment is different from that in the first embodiment, specifically shown in Fig. 2.

[0201] Note that each of all ciphers C5, C6, and C7 can be assigned with the same value or any optional value according to the suitable resistance of cipher necessary to protect the information unit against unfair access thereto. Similarly, each of all encryption system CS5, CS6, and CS7 can be selected from the identical encryption system or various different encryption system such as examples referred in the above. Furthermore, all ciphers and encryption system can be selected from those selected in the first embodiment.

Decoding encrypted multiple information unit into information unit

[0202] The encrypted information encrypted with ciphers in hierarchically arranged by the transmitting unit 510 can be decrypted by repeatedly using a single of descrambler with a simply constructed apparatus, which will be specifically described below. The encrypted multiple information unit Ime0b is supplied to the receiving unit 530 through the transmitter 120 in the format of transmission information It.

[0203] The receiver 131 of the receiving unit 530 takes out a part or the whole of encrypted multiple information Ime0b from the received transmission information It at step S701. At step S702, the descrambler 532 decrypts the received encrypted multiple information Ime0b with the seventh predetermined cipher C7 to obtain the multiple information unit Im1234b (not shown) constructed by the encrypted information unit Iue12b, the information unit Iu3b, and the encrypted information unit Iue4b. Note that thus obtained multiple information unit Im1234b can be produced in a format different from that of the multiple information unit Im1234b produced by the multiplexer 113 at Step S603.

[0204] The demultiplexer 533 demultiplexes the multiple information unit Im1234b produced at step S603, and separates each of encrypted information unit Iue and information unit Iu therefrom at step S703. Thus, the encrypted information unit Iue12b, the information unit Iu3b, and the encrypted information unit Iue4b are produced at step S703. Note that thus obtained information units Iue12b, Iu3b, and Iue4b can be produced in the formats different from those produced by the information unit scrambler 512 of the transmitting unit 510. Needless to say that those information units Iue12b, Iu3b, and Iue4b can be in the same formats as those produced by the information unit scrambler 512 of the transmitting unit 510, resulting in the reproduction of those information units Iue12b, Iu3b, and Iue4b.

[0205] The encrypted information unit Iue12b is sent to the descrambler 532 where the multiple information unit Im12b (not shown) is produced by decrypting the encrypted information unit Iue12b with the fifth predetermined cipher C5 at step S704. Thus produced multiple information unit Im12b is sent back to the demultiplexer 533 where the information units Iu1b and Iu2b are produced by demultiplexing the multiple information unit Im12b at step S703. Similarly, the encrypted information unit Iue4b is sent to the descrambler 532, where the information unit Iu4b is produced at step S704.

[0206] Each of information units Iu1b produced at step S703, Iu2b produced at step S703, Iu3b produced at step S703, and Iu4b produced at step S704 are sent to the reproducer 135, where the reproduction information Ir are produced from those information units Iu1b, Iu2b, Iu3b, and Iu4b at step S705. Note that all information units Iu1b, Iu2b, Iu3b, and Iu4b can be produced in the substantially same in content as those produced by the information unit generator 111, but can be different in the encrypting format or encrypting method. Of course, it is also possible to reproduce the completely same information units as those Iu1b, Iu2b, Iu3b, and Iu4b produced by the information unit generator 111.

[0207] With reference to Fig. 9, an alternative of the information transmission apparatus 500 of Fig. 5 is shown. The information transmission apparatus 500R shown in Fig. 9 has a construction where the lower layer scrambler 114 is removed from the information transmission apparatus 500. In this apparatus, the encryption for a lower layer transmission is performed not by the lower layer scrambler 114 (Fig. 5) but by the information unit scrambler 512 (Fig. 9). Therefore information unit scrambler 512 only have to encrypt under a certain encryption system used by a lower layer such as being performed by the transmitter 120. Needless to say, the information unit scrambler 512 may be able to encrypt under various encryption systems including one suitable for the above mentioned lower layer transmission.

(Third Embodiment)

[0208] With reference to Figs. 10, 11, and 12, an information transmission apparatus according to a third embodiment of the present invention is described. In this embodiment, the information transmission apparatus 800 includes a transmitting unit 810, transmitter 120, and a receiving unit 830. Here below, descriptions of any of substantially the same components constructing the information transmission apparatuses 100, 500, or 500R are generally omitted for reducing the redundancy.

[0209] Note that, the encrypted multiple information Ime produced by the descrambler 832 is substantially the same in content as the encrypted multiple information Ime produced by the lower layer scrambler 114 of the transmitting unit 810, but can be different in the encrypting format or encryption method. Of course, it is also possible to reproduce the completely same encrypted multiple information Ime as that produced by the lower layer scrambler 114.

Transmitting unit 810

[0210] The transmitting unit 810 has a construction substantially the same as that of the transmitting unit 510 already described with reference to Fig. 5. However, the operation of the transmitting unit 810 for producing the encrypted multiple information Ime is different from that of the transmitting unit 510, which will be described later with reference to Fig. 11 and Fig. 12.

Receiving unit 830

[0211] The receiving unit 830 has a construction similar to that of the receiving unit 530 shown in Fig. 5, such that the descrambler 532 and the demultiplexer 533 are replaced by a descrambler 832 and a demultiplexer 833. The descrambler 832 is connected to the receiver 131 for receiving the encrypted multiple information unit Ime therefrom. Then, the descrambler 832 decrypts the encrypted multiple information Ime once, and produce the multiple information unit Im. Note that the descrambler 832 can decrypt hierarchically and repeatedly encrypted multiple information unit. The descrambler 832 encrypts an information unit which is encrypted n (n is an integer) times and produced n-1 times encrypted information unit. Therefore, according to encryption times of the encrypted multiple information unit Ime inputted from the receiver 131, the descrambler 832 repeatedly decrypts the unit Ime till obtaining no more encrypted multiple information unit Ime.

[0212] The demultiplexer 833 is connected to the descrambler 832 for receiving the multiple information

Im therefrom, and demultiplexes the received multiple information Im to produce the information unit Iu. However, when the multiple information Im produced by the descrambler 832 includes the encrypted information unit Iue therein, the encrypted information unit Iue is sent back to the descrambler 832.

In Operation

[0213] With reference to Fig. 12, general operations performed by the receiving unit 830 of information transmission apparatus 800 will be described bellow. As described in the above, the transmitting unit 810 is substantially the same as the transmitting unit 510 in construction, therefore the generation operation is also substantially the same as those described with reference to Fig. 7.

[0214] The general operation of the receiving unit 830 is as follows.

[0215] At step S901, the receiver 131 receives the transmission information It from the transmitter 120, and takes out a part or the whole of encrypted multiple information Ime from the inputted transmission information It.

[0216] At step S902, the descrambler 832 receives the encrypted multiple information Ime produced at step S901. Then, the descrambler 832 decrypts the inputted encrypted multiple information Ime, and outputs the decryption results as the multiple information Im.

[0217] At step S903, the demultiplexer 833 separates the multiple information Im produced at step S902 for each encrypted information unit Iue, and takes out the encrypted information unit Iue and/or the information unit Iu.

[0218] At step S904, it is judged whether an information unit Iu outputted from the descrambler 832 or the demultiplexer 833 is encrypted or not. When it is judged "YES", meaning that the information unit Iu is encrypted, the information unit Iu (Iue) from the descrambler 832 or demultiplexer 833 is sent back to the descrambler 832. Then, the procedure advances to step S905.

[0219] However, when it is judged "NO", meaning that the information unit Iu outputted from the descrambler 832 or the demultiplexer 833 is no more encrypted. The information unit Iu from the descrambler 832 or demultiplexer 833 is sent to the reproducer 135. Then, the procedure advances to step S906.

[0220] At step S905, the descrambler 832 once decrypts the encrypted information unit Iue, and outputs the decryption result therefrom. Then the procedure returns to step S903. By repeatedly carrying out steps S903, S904, and S905, the descrambler 832 can decrypt the information unit Iu to be finally taken out, and take out the information unit Iu in a format which is not encrypted.

[0221] At step S906, the reproducer 135 receives the information unit Iu outputted by the descrambler 832 and/or the demultiplexer 833, and produces the reproduction information Ir.

[0222] At step S907, the presenter 136 presents the contents of reproduction information Ir obtained at step S906 to a user in accordance with the format of the reproduction information. Then, the procedure advances to step S903.

[0223] As described in the foregoing, the recursive encryption is performed a plurality of times in the information unit scrambler 512. The same cipher system as that used in the information unit scrambler 512 is used in the lower layer scrambler 114. Thus, it possible for the descrambler 832 to perform decryption corresponding to all the plurality of times of encryption.

Encoding information units into encrypted multiple information unit

[0224] With reference to Fig. 11 very similar to Fig. 2, the encrypted multiple information unit Ime produced by the information transmission apparatus 800 is described. The output from the lower layer scrambler 114, represented by a rectangle of a dot line, is the encrypted multiple information Ime0c.

[0225] The four outputs from the information unit generator 111, indicated by circles, are the information units Iu1c, Iu2c, Iu3c, and Iu4c, respectively. These information units Iu1c, Iu2c, Iu3c and Iu4c represent, for example, a tourist resort guide considering the weather forecast, a weather forecast for the tourist resort, a weather forecast for allover the country, and a weather forecast for a local area, respectively.

[0226] The rectangles Iue1c, Iue12c, and Iue4c each indicated by a dot line represent the units of encrypted information produced inside the transmitting unit 810 of the information transmission apparatus 800 at respective encryption stages. Specifically, the rectangle Iue1c represents an formation unit Iue which is produced, such that the information unit scrambler 512 encrypts the information unit Iu1c outputted from the information unit generator 111 with an eighth predetermined cipher C8 under an eighth predetermined encryption system CS8. Thus, the encrypted information unit Iue1c is produced.

[0227] The rectangle Iue12c represents also an encrypted information unit Iue which is produced at the following two steps. First, the multiplexer 113 multiplexes the first encrypted information unit Iue1c received from the information unit scrambler 512 and the information unit Iu2c, and produces a multiple information unit Im12c (not shown). Second, the information unit scrambler 512 encrypts the multiple information unit Im12c received from the multiplexer 113 with a ninth predetermined cipher C9 under a ninth predetermined encryption system CS9. Thus, the encrypted information unit Iue12c wherein the information unit Iu1c is encrypted twice is produced.

[0228] The rectangle Iue4c represents an encrypted information unit Iue which is produced,.such that the information unit scrambler 512 encrypts the information unit Iu4c outputted from the information unit generator 111 with a tenth predetermined cipher C10 under a tenth encryption system CS10. Thus, the encrypted information Iue4c is produced.

[0229] The rectangle Ime0c represents an encrypted multiple information Ime which is produced as follows. First, the multiplexer 113 multiplexes the encrypted information unit Iue12c, the information unit Iu3c, and the encrypted information unit Iue4c, and produces a multiple information unit Im1234c (not shown). Second, the lower layer scrambler 114 encrypts the multiple information unit Im1234 with a eleventh predetermined cipher C11 under a eleventh predetermined encryption system CS11.

[0230] As a result, the information unit Iu1c is encrypted thrice with the eighth, ninth, and eleventh predetermined ciphers C8, C9, and C11. The information unit Iu2c is encrypted twice with the ninth and eleventh predetermined ciphers C9, and C11. The information unit Iu3c is encrypted once with the eleventh predetermined cipher C11. The information unit Iu4c is encrypted twice with the tenth and eleventh predetermined ciphers C10 and C11.

[0231] Note that each of all ciphers C8, C9, C10, and C11 can be assigned with the same value or any optional value according to the suitable resistance of cipher necessary to protect the information unit against unfair access thereto. Similarly, each of all encryption system CS8, CS9, CS10, and CS11 can be selected from the identical encryption system or various different encryption system such as examples referred in the above. Furthermore, all ciphers and encryption system can be selected from those selected in the first and second embodiments.

Decoding encrypted multiple information unit into information unit

[0232] The encrypted information encrypted with ciphers in hierarchically arranged by the transmitting unit 810 can be decrypted by repeatedly using a single of descrambler with a simply constructed apparatus, which will be specifically described below. The encrypted multiple information unit Ime0c is supplied to the receiving unit 830 through the transmitter 120 in the format of transmission information It.

[0233] The receiver 131 of the receiving unit 830 takes out a part or the whole of encrypted multiple information Ime0c from the received transmission information It at step S901. At step S902, the descrambler 832 decrypts the received encrypted multiple information Ime0c with the eleventh predetermined cipher C11 to obtain the multiple information unit Im1234c (not shown) constructed by the encrypted information unit Iue12c, the information unit Iu3c, and the encrypted information unit Iue4c. Note that thus obtained multiple information unit Im1234c can be produced in a format different from that of the multiple information unit Im1234c produced by the multiplexer 113.

[0234] The demultiplexer 133 demultiplexes the multiple information unit Im1234c produced at step S902, and separates each of encrypted information unit Iue and/or information unit Iu therefrom at step S903. Thus, the encrypted information unit Iue12c, the information unit Iu3c, and the encrypted information unit Iue4c are produced at step S903. Note that thus obtained information units Iue12c, Iu3c, and Iue4c can be produced in the formats different from those produced by the information unit scrambler 512 of the transmitting unit 810. Needless to say that those information units Iue12c, Iu3c, and Iue4c can be in the same formats as those produced by the information unit scrambler 512 of the transmitting unit 810, resulting in the reproduction of those information units Iue12c, Iu3c, and Iue4c.

[0235] Trough the operations performed at steps S904 and S905, the reproduction information Ir are produced from those information units Iu1c, Iu2c, Iu3c, and Iu4a at step S906. Note that all information units Iu1c, Iu2c, Iu3c, and Iu4a can be produced in the substantially same in content as those produced by the information unit generator 111, but can be different in the encrypting format or encrypting method. Of course, it is also possible to reproduce the completely same information units as those Iu1c, Iu2c, Iu3c, and Iu4c produced by the information unit generator 111.

[0236] With reference to Fig. 13, an alternative of the information transmission apparatus 800 of Fig. 10 is shown. The information transmission apparatus 800R shown in Fig. 13 has a construction where the lower layer scrambler 114 is removed from the information transmission apparatus 800. In this apparatus, the encryption for a lower layer transmission is performed not by the lower layer scrambler 114 (Fig. 10) but by the information unit scrambler 512 (Fig. 14). Therefore information unit scrambler 512 only have to encrypt under a certain encryption system used by a lower layer such as being performed by the transmitter 120. Needless to say, the information unit scrambler 512 may be able to encrypt under various encryption systems including one suitable for the above mentioned lower layer transmission.

(Fourth Embodiment)

[0237] With reference to Figs. 14, 15, 16, and 17, an information transmission apparatus according to the fourth embodiment of the present invention is described here below. The information transmission apparatus 1000 includes a transmitting unit 1010, the transmitter 120, and a receiving unit 1030. Here below, descriptions of any of substantially the same components constructing the information transmission apparatuses 100, 500, 500R, 800, or 800R are generally omitted for reducing the redundancy.

Transmitting unit 1010

[0238] The transmitting unit 1010 has a construction very similar to that of the transmitting unit 110 of the first embodiment, such that the information unit scrambler 112 is replaced by an information unit scrambler 1012. The information unit scrambler 1012 recursively encrypts the information units Iu outputted by the information unit generator 111 a plurality of times, and produces the encrypted information units Iue. A method of performing recursive encryption a plurality of times may be the same as that performed by the information unit scrambler 112 in the first embodiment.

[0239] The information unit scrambler 1012 adds an encrypted information unit Identifier which is an identifier for distinguishing an information unit Iu from the outputted encrypted information units Iue. Hereinafter the encrypted information unit Identifier is hereinafter referred to as an encrypted information unit ID for simplification. Although the encrypted information unit Iue is composed of so-called child encrypted information units Iue, the encrypted information unit ID shall be added not to the child encrypted information units Iue but to parent encrypted information units Iue. The same value is assigned to information units Iu updated with time as the encrypted information unit ID. For example, the same encrypted information unit ID is assigned to an information unit Iu of the weather in allover the country for yesterday and an information unit Iu of the weather in allover the country for today.

Receiving Unit 1030

[0240] The receiving unit 1030 includes receiver 131, a lower layer descrambler 132, demultiplexer 1033, storage 1034, an information unit descrambler 1035, reproducer 1036, and presenter 136. Specifically the receiving unit 1030 has a construction similar to that of the receiving unit 130 of the first embodiment shown in Fig. 1, such that the demultiplexer 133 and reproducer 135 are replaced by the demultiplexer 1033 and the reproducer 1036, respectively, in this embodiment.

[0241] Furthermore, the storage 1034 is additionally inserted between the demultiplexer 1033 and the reproducer 1036. The storage 1034 is connected to the demultiplexer 1033 and the reproducer 1036 for receiving the encrypted information unit Iue and an reproduction designating information Idr therefrom, respectively. The storage 1034 is further connected to the information unit descrambler 1035 for exchanging the encrypted information unit Iue therebetween.

[0242] The storage 1034 stores the encrypted information unit Iue inputted from the demultiplexer 1033 and the information unit descrambler 1035 therein. Then, the storage 1034 replaces the encrypted information Iue therein with newly inputted encrypted information Iue which is being updated. Thus, the encrypted information unit Iue stored in the storage is updated to the newest one. When the stored encrypted information unit Iue is designated by the inputted reproduction designating information Idr, the storage 1034 outputs the encrypted information unit Iue.

[0243] The information unit descrambler 1035 is further connected to the input port thereof for supplying an encrypted information unit Iue (an information unit Iu which is not encrypted is also an encrypted information unit Iue, as defined previously). The information unit descrambler 1035 is also connected to the input port of the demultiplexer 1033 for supplying an encrypted information unit Iue.

[0244] The reproducer 1036 is further connected to the demultiplexer 1033 for receiving the information unit Iu therefrom, and produces the reproduction information Ir and the reproduction designating information Idr. The reproduction designating information Idr is an information for designating an information unit Iu. Specifically, the reproduction designating information Idr designates the information unit Iu included in the encrypted information unit Iue stored in the storage 1034. The information unit Iu designated by the reproduction designating information Idr may be determined by a user's direct entry, or may be determined independently by the information transmission apparatus 1000 itself.

[0245] The presenter 136 is connected to the reproducer 1036 for receiving the reproduction information Ir therefrom. Then, the presenter 136 presents contents included in the reproduction information Ir to a user.

In Operation

[0246] With reference to Figs. 15, 16, and 17, the operations performed by the information transmission apparatus 1000 is described below.

[0247] In Fig. 15, a flow chart showing the operations performed by the transmitting unit 1010 and the transmitter 120 is shown.

[0248] At step S1101, the information unit generator 111 produces a plurality of information units Iu.

[0249] At step S1102, the information unit scrambler 1012 recursively encrypts the information units Iu generated at step S1101, and takes the results thereof as encrypted information units Iue.

[0250] At step S1103, an encrypted information unit ID is added to the encrypted information units Iue generated at step S1102. The encrypted information unit ID can be easily taken out without decrypting the encrypted information unit Iue because it is added to the result of encrypting the information unit Iu at step S1102.

[0251] At step S1104, the multiplexer 113 multiplexes the encrypted information units Iue generated by the encryption at step S1103, and outputs the result thereof as multiple information Im.

[0252] At step S1105, the lower layer scrambler 114 encrypts the multiple information Im obtained by the multiplying at step S1104, and produces the encrypted multiple information Ime. The encryption performed at step S1105 shall use the same cipher as that used in the encryption performed at step S1102.

[0253] At step S1106, the sender 115 converts the encrypted multiple information Ime obtained by the encryption at step S1105 into a format which is suitable for transmission by the transmitter 120, and produces the transmission information It.

[0254] At step S1107, the transmitter 120 transmits the transmission information It to a physically distant point. In this case, a plurality of receiving units 1030 may correspond to one transmitting unit 1010.

[0255] In Fig. 16, a flow chart showing the operation performed by the receiving unit 1030 is shown.

[0256] At step S1201, the receiver 131 receives the transmission information It from the transmitter 120, and takes out a part or the whole of encrypted multiple information Ime from the inputted transmission information It.

[0257] At step S1202, the lower layer descrambler 132 receives the encrypted multiple information Ime obtained at step S1201, and decrypts the inputted encrypted multiple information Ime.

[0258] At step S1203, the demultiplexer 1033 separates the multiple information Im obtained at step S1202 for each encrypted information unit Iue, and takes out the encrypted information unit Iue.

[0259] At step S1204, the storage 1034 stores the encrypted information unit Iue using the encrypted information unit ID.

[0260] In Fig. 17, the details of the operations performed by the storage 1034 at step S1204 will be described below.

[0261] At step S1301, an encrypted information unit Iue is inputted from the demultiplexer 1033.

[0262] At step S1302, a value i of an encrypted information unit ID added to the encrypted information unit Iue inputted at step S1301 is obtained.

[0263] At step S1303, it is examined by retrieval whether or not the encrypted information unit Iue, to which the encrypted information unit ID having the value i is added, has been already stored in the storage 1034.

[0264] At step S1304, It is judged whether any encrypted information unit Iue is stored in the storage 1034 or not. When it is judged "YES", the procedure advances to step S1305. However, when it s judged "NO", the procedure advances to step S1306.

[0265] At step S1305, the encrypted information unit Iue inputted at step S1301 is added and stored. Thereafter, the procedure returns to step S1301. From step S1301, the processing is repeated.

[0266] At step S1306, the encrypted information unit Iue, to which the encrypted information unit ID having the value i is added, currently stored is removed, and the encrypted information unit Iue inputted at step S1301 is stored instead. Thereafter, the procedure returns to step S1301. From step S1301, the processing is repeated.

[0267] As described in the foregoing, the information unit Iu stored in the storage 1034 is encrypted as an encrypted information unit Iue. Even if the contents of the storage 1034 is unfairly referred to, therefore, the secrecy is ensured. In the case of updating, the encrypted information unit ID is assigned to the parent encrypted information units Iue, thereby making it easy to take out the encrypted information unit ID from the encrypted information unit Iue outputted by the demultiplexer 1033. The encrypted information unit ID which can be easily taken out is only used, so that it is very simply feasible to perform updating processing of the contents of the storage 1034.

[0268] By adding an information indicating whether or not updating is performed to the encrypted information unit ID, it is possible to simplify processing of the encrypted information unit Iue sent many times without being changed by the storage 1034. As examples of the information indicating whether or not updating is performed are;

(1) a flag indicating that updating is performed,
(2) a numerical value representing a version, and
(3) a checksum of the whole of information are considered.

[0269] At step S1205, the procedure advances to step S1206 when the reproducer 1036 outputs reproduction designating information Idr, while being returned to step S1201 when it does not output the reproduction designating information Idr.

[0270] At step S1206, the storage 1034 takes out the encrypted information unit Iue having the encrypted information unit ID designated by the reproduction designating information Idr outputted at step S1205 from the storage 1034. Then, the storage 1034 outputs the encrypted information unit Iue.

[0271] At step S1207, when an information unit Iu to be taken out exists in a state where it is not encrypted in the encrypted information unit Iue inputted to the information unit descrambler 1035, the procedure advances to step S1209.

[0272] At step S1208, the information unit descrambler 1035 decrypts once the encrypted information unit Iue in which there exists the information unit Iu to be taken out. Thereafter, the procedure returns to step S1207. At step S1209, the reproducer 1036 receives the information unit Iu outputted by the information unit descrambler 1035. Then, the reproducer 1036 generates the reproduction information Ir.

[0273] At step S1210, the presenter 136 presents the reproduction information obtained at step S1209 to a user in accordance with the format of the reproduction information.

[0274] As described in the foregoing, the encrypted information unit ID is added to the encrypted information unit Iue. Additionally provided is the storage 1034. Thus, the encrypted information unit Iue stored in the storage 1034 can be updated to the newest one without performing decryption processing in the information unit descrambler 1035. When the user actually views the encrypted information unit Iue, the encrypted information unit Iue is decrypted by the information unit descrambler 1035.

[0275] It is to be noted that the information unit descrambler 134 used in the foregoing embodiments should be able to decrypts the multiple encrypted information unit Iu (Ime) at the same time. Contrary, the information unit descrambler 1035 is free from such a restriction peculiar to the information unit descrambler 134, owing to that the encrypted information which is a result of one time decryption. Specifically, by receiving the information little by little from the storage 1034, it is possible to decrypts the encrypted information at slower processing speed compared with the speed at which the transmitter 120 transmits.

[0276] Furthermore, it is also possible to temporarily outputs the encrypted information unit Iue into the storage 1034, only when the processing can not be completed within a determined period. This temporarily stored encrypted information is outputted to the information unit descrambler 1035, and then is processed thereat.

[0277] As described in the above, a result of that the encrypted information unit Iue is little by little supplied from the storage 1034 to the information unit descrambler 1035, and then thus supplied encrypted information unit Iue is little by little outputted from the information unit descrambler 1035. Resultantly, the demultiplexer 1033 may demultiplex to dissolve the multiplexed information into each information unit at a slower speed compared with a transmission speed by the transmitter 120.

[0278] The reproducer 1036 designates the contents of information to be supplied to the storage 1034 in accordance with the user's request. For this purpose, the reproducer 1036 produces the reproduction designating information Idr. Owing to this reproduction designating information Idr, it is possible to perform decryption at any optional timing. Thus, even if the encryption key is supplied later than the encrypted information (It), the receiving unit 1030 can process that encrypted information.

(Fifth Embodiment)

[0279] With reference to Figs. 18, 19, and 20, an information transmission apparatus according to the fifth embodiment of the present invention is described. The information transmission apparatus 1400 includes a transmitting unit 1410, the transmitter 120, and a receiving unit 1430. Here below, descriptions of any of substantially the same components constructing the information transmission apparatuses 100, 500, 500R, 800, 800R, or 1000 are generally omitted for reducing the redundancy.

[0280] The information transmission apparatus 1400 is constructed by removing such a restriction that the information unit scrambler 1012 recursively encrypts a plurality of times from the information transmission apparatus 1000 according to the fourth embodiment. Furthermore, the lower layer descrambler 132 and the information unit descrambler 1035 in the fourth embodiment are integrated into the descrambler 1432 in the fifth embodiment. It can be considered that the integration enables the descrambler 1432 to substitute for the function of the information unit descrambler 1035.

Transmitting unit 1410

[0281] The transmitting unit 1410 has a construction substantially the same as that of the transmitting unit 1010 shown in Fig. 14. Therefore, description is omitted.

Receiving unit 1430

[0282] The receiving unit 1430 has a construction very similar to that of the receiving unit 1030, such that the lower layer descrambler 132 and the information unit descrambler 1035 are replaced by a descrambler 1432.

[0283] The descrambler 1432 is connected to the receiver 131 and the storage 1034 for receiving the multiple information units Iue therefrom. Then, the descrambler 1432 outputs multiple information Im, when the encrypted multiple information Ime is inputted thereto. Further, the descrambler 1432 decrypts, when the encrypted information unit Iue is inputted thereto, the inputted encrypted information unit Iue, and outputs an information unit Iu which is the decryption result thereof. Thus obtained information unit Iu is directly supplied to the reproducer 1036.

[0284] The demultiplexer 1433 is connected to the descrambler 1432 for receiving the multiple information unit Im therefrom to demultiplex the received multiple information unit Im. Then, the demultiplexer 1433 produces the encrypted information unit Iue and send it to the storage 1034, when the multiple information unit Im from the descrambler 1432 is encrypted. The demultiplexer 1433 produces the information unit Iu and send it to the reproducer 1036, when the multiple information unit Im from the descrambler 1432 is not encrypted.

[0285] The storage 1034 is connected to the demultiplexer 1433 and the reproducer 1036 for receiving the encrypted information unit Iue and reproduction designating information Idr therefrom, respectively. The storage 1034 is further connected to the input port of the descrambler 1432. The storage 1034 stores the received encrypted information unit Iue therein, and replaces the stored encrypted information unit Iue when the encrypted information unit Iue is updated. Thus, the encrypted information unit Iue stored in the storage 1034 is kept the newest.

[0286] When the stored encrypted information unit Iue is designated by the received reproduction designating information Idr, the storage 1034 outputs the encrypted information unit Iue. This encrypted information unit Iue is directly fed back to the descrambler 1432.

[0287] The reproducer 1036 is connected to the demultiplexer 1433 for receiving the information unit Iu therefrom, and to the storage 1034 for supplying the reproduction designating information Idr thereto.

[0288] Note that descrambler 1432 can perform the decryption process at slower speed not conforming to the information transmission speed at the transmitter 120, owing to that the encrypted information Iue is supplied to the descrambler 1432 from the storage 1034 little by little. This is especially effective for the first and more inner, viewed from the outer shell, encrypted and more inner encrypted information units.

[0289] As described in the above, a result of that the encrypted information unit Iue is little by little supplied from the storage 1034 to the descrambler 1432. Resultantly, the demultiplexer 1433 may demultiplex to dissolve the first and more inner, viewed from the outer shell, multiplexed information units and at a slower speed compared with a transmission speed by the transmitter 120.

In Operation

[0290] With reference to Figs. 19 and 20, the operations of the information transmission apparatus 1400 is described briefly. In Fig. 19, a flow chart for operations performed by the transmitting unit 1410 and the transmitting unit 120 is shown.

[0291] At step S1501, the information unit generator 111 produces a plurality of information units Iu, and outputs the generated information units Iu.

[0292] At step S1502, the information unit scrambler 1012 respectively encrypts the information units Iu generated at step S1501, and takes the results thereof as encrypted information units Iue.

[0293] At step S1503, an encrypted information unit ID is added to the encrypted information units Iue generated at step S1502.

[0294] At step S1504, the multiplexer 113 multiplexes the encrypted information units Iue generated by the encryption at step S1502, and outputs the result thereof as multiple information Im.

[0295] At step S1505, the lower layer scrambler 114 encrypts the multiple information Im obtained by the multiplexing at step S1504, and produces the encrypted multiple information Ime. The encryption performed by the lower layer scrambler 114 shall use the same cipher as that in the encryption performed by the information unit scrambler 1012.

[0296] At step S1506, the sender 115 converts the encrypted multiple information Ime obtained by the encryption at step S1505 into a format which is suitable for transmission by the transmitter 120, and produces the transmission information It. At step S1507, the transmitter 120 transmits the transmission information It to a physically distant point. In this case, a plurality of receiving units 1430 may correspond to one transmitting unit 1410.

[0297] In Fig. 20, a flow chart for operations performed by the receiving unit 1430 is shown.

[0298] At step 1601, the receiver 131 receives the transmission information It inputted from the transmitter 120, and takes out a part or the whole of encrypted multiple information Ime from the inputted transmission information It.

[0299] At step S1602, the descrambler 1432 receives the encrypted multiple information Ime obtained at step S1601. Then, the descrambler 1432 decrypts the received encrypted multiple information Ime, and produces the multiple information Im.

[0300] At step S1603, the multiplexer 1433 separates the multiple information Im obtained at step S1602 for each encrypted information unit Iue, and takes out the encrypted information unit Iue.

[0301] At step S1604, the storage 1034 stores the encrypted information unit Iue using the encrypted information unit ID.

[0302] At step S1605, the procedure advances to step S1606 when the reproducer 1036 outputs reproduction designating information Idr, while being returned to step S1601, when it does not output the reproduction designating information Idr.

[0303] At step S1606, the storage 1034 takes out the encrypted information unit Iue having the encrypted information unit ID designated by the reproduction designating information Idr outputted at step S1605 from the storage 1034. Then, the storage 1034 outputs the encrypted information unit Iue.

[0304] At step S1607, the descrambler 1432 decrypts the encrypted information unit Iue, to generate an information unit Iu. When the information unit Iu is encrypted once, the encrypted information unit Iue is decrypted once, thereby making it possible to generate an information unit Iu. Although, there is such a restriction that the information unit Iu is recursively encrypted a plurality of times in the fourth invention, the restriction is not placed in this invention.

[0305] At step S1608, the reproducer 1435 receives the information unit Iu outputted by the descrambler 1432, and produces the reproduction information Ir.

[0306] At step S1609, the presenter 1436 presents the reproduction information obtained at step S1608 to a user in accordance with the format of the reproduction information.

[0307] As described in the foregoing, the encryption performed by the information unit scrambler 1012 is made the same as the encryption performed by the lower layer scrambler 114. Thus, it possible for the single descrambler 1432 to decode a cipher used in not only the lower layer scrambler 114 but also the information unit scrambler 1012. That is, it is possible to decrypt the information unit Iu by preparing only one descrambler which is not special.

[0308] Further, the encrypted information unit ID is added to the encrypted information unit Iue, and the storage 1034 is added, thereby making it possible to update the encrypted information unit Iue stored in the storage 1034 to the newest one without performing decryption processing in the descrambler 1432. When the user actually views the encrypted information unit Iue, the encrypted information unit Iue is decrypted by the descrambler 1432.

[0309] With reference to Fig. 21, an alternative of the information transmission apparatus 1400 of Fig. 18 is shown. The information transmission apparatus 1400R shown in Fig. 21 has a construction where the lower layer scrambler 114 is removed from the information transmission apparatus 1400. In this apparatus, the encryption for a lower layer transmission is performed not by the lower layer scrambler 114 (Fig. 18) but by the information unit scrambler 1012 (Fig. 21). Therefore information unit scrambler 1012 only have to encrypt under a certain encryption system used by a lower layer such as being performed by the transmitter 120. Needless to say, the information unit scrambler 1012 may be able to encrypt under various encryption systems including one suitable for the above mentioned lower layer transmission.

(Sixth Embodiment)

[0310] With reference to Figs. 22, 23, and 25, an information transmission apparatus according to the sixth embodiment of the present invention is described. The information transmission apparatus 1700 includes a transmitting unit 1710, the transmitter 120, and a receiving unit 1730. Here below, descriptions of any of substantially the same components constructing the information transmission apparatuses 100, 500, 500R, 800, 800R, 1000, 1400, and 1400R are generally omitted for reducing the redundancy.

[0311] In this embodiment, it is invented that the information unit Iu which is outputted from the descrambler 1732 is supplied back thereto, so that the descrambler 1732 can handle such information unit as been recursively encrypted a plurality of times.

Transmitting unit 1710

[0312] The transmitting unit 1710 has a construction substantially the same as that of the transmitting unit 1010 shown in Fig. 14. Therefore, description is omitted.

Receiving unit 1730

[0313] The receiving unit 1730 has a construction very similar to that of the receiving unit 1430 according to the fifth embodiment (Fig. 18), such that the descrambler 1432 is replaced by a descrambler 1732.

[0314] The descrambler 1732 is connected to the receiver 131 for receiving the encrypted multiple information Ime therefrom, and produces the encrypted information unit Iue, the multiple information Im, or the information unit Iu. The descrambler 1732 has a loop line for returning thus produced encrypted information unit Iue thereto. The descrambler 1732 is also connected to the reproducer 1036 for supplying thus produced information unit Iu thereto, and to the demultiplexer 1433 for supplying thus produced multiple information Iu thereto. Further, the descrambler 1732 is bilaterally connected to the storage 1034 for exchanging the encrypted information unit Iue therebetween.

The descrambler 1732 outputs, when the encrypted multiple information Ime is inputted thereto, multiple information Im, while decrypting, when the encrypted information unit Iue is inputted thereto, the encrypted information unit Iue, and outputs an information unit Iu which is the result thereof.

[0315] The demultiplexer 1433 is connected to the descrambler 1732 for receiving the multiple information Im therefrom, and outputs an encrypted information unit Iue and/or the information unit Iu.

[0316] The storage 1034 receives the encrypted information unit Iue outputted by the demultiplexer 1433 and demultiplexer 1732, and the reproduction designating information Idr outputted by the reproducer 1036. Then, the storage 1034 also outputs the encrypted information unit Iue to the descrambler 1732.

[0317] The storage 1034 stores the received encrypted information unit Iue, and replaces, when the encrypted information unit Iue is updated, the stored encrypted information unit Iue, to update the encrypted information unit Iue to the newest one.

[0318] When the stored encrypted information unit Iue is designated by the received reproduction designating information Idr, the storage 1034 outputs the encrypted information unit Iue.

[0319] The reproducer 1036 receives the information unit Iu outputted by the descrambler 1732, and outputs the reproduction information Ir and the reproduction designating information Idr. It is to be noted that the descrambler 832 used in the third embodiment should be able to decrypts the multiple encrypted information unit Iu at the same time. Contrary, the descrambler 1732 is free from such a restriction that the descrambler 832, owing to that the encrypted information which is a result of one time decryption is temporarily stored in the storage 1034.

[0320] Furthermore, it is also possible to temporarily outputs the encrypted information unit Iue into the storage 1034, only when the processing can not be completed within a determined period. This temporarily stored encrypted information is outputted to the information unit descrambler 1732, and then is processed thereat.

In Operation

[0321] With reference to Fig. 23, the operations performed by the receiving unit 1730 will be described in detail.

[0322] At step S1801, the receiver 131 receives the transmission information It from the transmitter 120, and takes out a part or the whole of the encrypted multiple information Ime from the received transmission information It.

[0323] At step S1802, the descrambler 1732 receives the encrypted multiple information Ime obtained at step S1801. Then, the descrambler 1732 decrypts the received encrypted multiple information Ime, and produces the multiple information Im.

[0324] At step S1803, the demultiplexer 1433 separates the multiple information Im obtained at step S1802 for each encrypted information unit Iue, and takes out the encrypted information unit Iue.

[0325] At step S1804, the storage 1034 stores the encrypted information unit Iue using the encrypted information unit ID.

[0326] At step S1805, the procedure advances to step S1806 when the reproducer 1036 outputs reproduction designating information Idr, while being returned to step S1801 when it does not output the reproduction designating information Idr.

[0327] At step S1806, the storage 1034 takes out the encrypted information unit Iue having the encrypted information unit ID designated by the reproduction designating information Idr outputted at step S1805 from the storage 1034 storing the encrypted information unit Iue, and outputs the encrypted information unit Iue taken out.

[0328] At step S1807, when an information unit Iu to be taken out exists in a state where it is not encrypted in the encrypted information unit Iue inputted to the descrambler 1732, the procedure advances to step S1809.

[0329] At step S1808, the descrambler 1732 decrypts once the encrypted information unit Iue in which there exists the information unit Iu to be taken out. Thereafter, the procedure returns to step S1807.

[0330] At step S1809, the reproducer 1036 receives the information unit Iu outputted by the descrambler 1732, and produces the reproduction information Ir which is reproducible information.

[0331] At step S1810, the reproducer 136 presents the reproduction information Ir obtained at step S1809 to a user in accordance with the format of the reproduction information.

[0332] As described in the foregoing, the recursive encryption is performed a plurality of times by the information unit scrambler 1012, and the same cipher system as that used in the information unit scrambler 1012 is used in the lower layer scrambler 114, thereby making it possible to perform decryption corresponding to all the plurality of times of encryption in the descrambler 1732.

[0333] Further, the encrypted information unit ID is added to the encrypted information unit Iue, and the storage 1034 is added, thereby making it possible to update the encrypted information unit Iue stored in the storage 1034 to the newest one without performing decryption processing in the descrambler 1732. When the user actually views the encrypted information unit Iue, the encrypted information unit Iue is decrypted by the descrambler 1732.

[0334] With reference to Fig. 24, an alternative of the information transmission apparatus 1700 of Fig. 22 is shown. The information transmission apparatus 1700R shown in Fig. 24 has a construction where the lower layer scrambler 114 is removed from the information transmission apparatus 1700. In this apparatus, the encryption for a lower layer transmission is performed not by the lower layer scrambler 114 (Fig. 22) but by the information unit scrambler 1012 (Fig. 24). Therefore information unit scrambler 1012 only have to encrypt under a certain encryption system used by a lower layer such as being performed by the transmitter 120. Needless to say, the information unit scrambler 1012 may be able to encrypt under various encryption systems including one suitable for the above mentioned lower layer transmission.

[0335] As described in detail in the foregoing, according to the present invention, information units Iu are subjected to the same recursive encryption a plurality of times, and are decrypted a plurality of times by one descrambler. Therefore, it is possible to not only perform encryption having a larger degree of freedom, as compared with that in the conventional example, but also to simplify the information transmission apparatus by preventing a special descrambler and the addition of a descrambler, for example.

[0336] Furthermore, an encrypted information unit ID added after the encryption of the information unit Iu is introduced, to update the contents of storage newly provided on the basis of the ID. In actually viewing the information unit Iu, the information unit Iu is decrypted by the descrambler. Therefore, it is not only feasible to simply manage the updating of the contents of the storage but also possible to prevent, because the stored information unit Iu is descrambled when it is viewed, users who do not pay fees from unfairly viewing the information unit Iu. Therefore, the present invention is high in affinity for a system of charging fees in the case of decryption.

[0337] While the invention has been described in detail, the foregoing description is in all aspects illustrative and not restrictive. It is understood that numerous other modifications and variations can be devised without departing from the scope of the invention.

Claims

1. An information transmission apparatus (110) in use for an information transmission system (100) where an encrypted information (It) comprised of a plural-

ity of information units (Iu) each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, said information (It) being encrypted for the transmission, said apparatus (110) comprising:

an information unit producing means (111) for producing said information unit (Iu);
a first encryption means (112) for encrypting said information unit (Iu) with a first predetermined encryption system to produce an encrypted information unit (Iue); and
a first multiplex means (113) for multiplexing at least one of said information unit (Iu) and said encrypted information unit (Iue) to produce a multiplexed information unit (Im) .

2. An information transmission apparatus (110) as claimed in Claim 1, further comprising:

a second encryption means (112) for encrypting said multiple information (Im) with a second predetermined encryption system to produce said encrypted multiplexed information (Iue); and
a second multiplex means (113) for multiplexing said encrypted information unit (Iue) to produce said multiplexed information (Im).

3. An information transmission apparatus (110) as claimed in Claim 2, further comprising:

a third encryption means (114) for encrypting said multiplexed information (Im) with a third predetermined encryption system to produce an encrypted multiple information unit (Ime).

4. An information transmission apparatus (510) as claimed in Claim 3, wherein said third predetermined encryption system is the same as that applied to said encrypted information (It).

5. An information transmission apparatus (510) as claimed in Claim 3, wherein said second predetermined encryption system is the same as said third predetermined encryption system.

6. An information transmission apparatus (510) as claimed in Claim 3, wherein said first, second, and third predetermined encryption systems are the same.

7. An information transmission apparatus (110) as claimed in Claim 1, further comprising:

a transmitting means (115) for converting said encrypted multiplexed information (Ime) into a format suitable for an efficient transmission.

8. An information transmission apparatus (510R) as claimed in Claim 1, wherein said first encryption means (512) encrypts said information unit (Iu) with an encryption system suitable for the transmission of information.

9. An information transmission apparatus (130) in use for an information transmission system (100) where an encrypted information (It) comprised of a plurality of information units (Iu) each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, said information (It) being encrypted for the transmission, said apparatus (110) comprising:

a first decryption means (132) for decrypting said encrypted information (It) with a first decryption system to produce a first multiplexed information unit (Im);
a first demultiplex means (133) for demultiplexing said first multiplexed information unit (Im) into any of a first encrypted information unit (Iue), a second multiplexed information unit (Iue) and said information unit (Iu); and
a second decryption means (134) for decrypting said first encrypted information unit (Iue) with a second decryption system to produce said information unit (Iu) or a second encrypted information unit (Iue).

10. An information transmission apparatus (130) as claimed in Claim 9, further comprising:

a second demultiplex means (133) for demultiplexing said second multiplexed information unit (Iue);
a third decryption means (132) for decrypting said second encrypted information unit (Iue) with a third predetermined decryption system to produce said information unit (Iu).

11. An information transmission apparatus (130) as claimed in Claim 9, wherein said first decryption system is the same as that applied to said encrypted information (It).

12. An information transmission apparatus (1030) as claimed in Claim 1, further comprising:

a storage means (1034) provided between said first demultiplexing means (1033) and said second decryption means (1035) for storing any of said first and second encrypted information units (Iue).

13. An information transmission apparatus (1030) as claimed in Claim 12, further comprising:

a reproducing means (1036) for receiving said encrypted information units (Iue) from said second decryption means (1035) to produce a reproduction information (Ir) indicating a content said encrypted information (It), said reproducing means (1036) requesting said storage means (1034) to supply said stored encryption information unit (Iue) to said second decryption means (1035).

14. An information transmission method for transmitting an encrypted information (It) comprised of a plurality of information units (Iu) each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, said information (It) being encrypted for the transmission, said method comprising the steps of:

producing (S301) said information unit (Iu);
encrypting (S302) said information unit (Iu) with a first predetermined encryption system to produce an encrypted information unit (Iue); and
multiplexing (S303) at least one of said information unit (Iu) and said encrypted information unit (Iue) to produce a multiplexed information unit (Im) .

15. An information transmission method as claimed in Claim 14, further comprising the steps of:

encrypting (S302) said multiple information (Im) with a second predetermined encryption system to produce said encrypted multiplexed information (Iue); and
multiplexing (S303) said encrypted information unit (Iue) to produce said multiplexed information (Im).

16. An information transmission method as claimed in Claim 15, further comprising:

encrypting (S304) said multiplexed information (Im) with a third predetermined encryption system to produce an encrypted multiple information unit (Ime).

17. An information transmission method as claimed in Claim 16, wherein said third predetermined encryption system is the same as that applied to said encrypted information (It).

18. An information transmission method as claimed in Claim 16, wherein said second predetermined encryption system is the same as said third predetermined encryption system.

19. An information transmission method as claimed in Claim 16, wherein said first, second, and third predetermined encryption systems are the same.

20. An information transmission method as claimed in Claim 14, further comprising the step of:

converting (S305) said encrypted multiplexed information (Ime) into a format suitable for an efficient transmission.

21. An information transmission method as claimed in Claim 14, wherein at said encrypting step (S302) said information unit (Iu) is encrypted with an encryption system suitable for the transmission of information.

22. An information transmission method for transmitting an encrypted information (It) comprised of a plurality of information units (Iu) each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, said information (It) being encrypted for the transmission, said method comprising the steps of:

decrypting (S402) said encrypted information (It) with a first decryption system to produce a first multiplexed information unit (Im);
demultiplexing (S403) said first multiplexed information unit (Im) into any of a first encrypted information unit (Iue), a second multiplexed information unit (Iue) and said information unit (Iu); and
decrypting (S405) said first encrypted information unit (Iue) with a second decryption system to produce said information unit (Iu) or a second encrypted information unit (Iue).

23. An information transmission method as claimed in Claim 22, further comprising the steps of:

demultiplexing (S404) said second multiplexed information unit (Iue);
decrypting (S405) said second encrypted information unit (Iue) with a third predetermined decryption system to produce said information unit (Iu).

24. An information transmission apparatus (130) as claimed in Claim 22, wherein said first decryption system is the same as that applied to said encrypted information (It).

25. An information transmission apparatus (1030) as claimed in Claim 14, further comprising the step of:

storing (S1204) any of said first and second encrypted information units (Iue).

26. An information transmission apparatus (1030) as claimed in Claim 25, further comprising the step of:

a reproducing means (1036) for receiving said encrypted information units (Iue) from said second decryption means (1035) to produce a reproduction information (Ir) indicating a content said encrypted information (It), said reproducing means (1036) requesting said storage means (1034) to supply said stored encryption information unit (Iue) to said second decryption means (1035).

27. An information transmission system (100) for transmitting an encrypted information (It) comprised of a plurality of information units (Iu) each hierarchically encrypted and multiplexed to each other is communicated between at least two parties, said information (It) being encrypted for the transmission, said system (100) comprising:

an information unit producing means (111) for producing said information unit (Iu);
a first encryption means (112) for encrypting said information unit (Iu) with a first predetermined encryption system to produce an encrypted information unit (Iue);
a first multiplex means (113) for multiplexing at least one of said information unit (Iu) and said encrypted information unit (Iue) to produce a multiplexed information unit (Im);
a first decryption means (132) for decrypting said encrypted information (It) with a first decryption system to produce a first multiplexed information unit (Im);
a first demultiplex means (133) for demultiplexing said first multiplexed information unit (Im) into any of a first encrypted information unit (Iue), a second multiplexed information unit (Iue) and said information unit (Iu); and
a second decryption means (134) for decrypting said first encrypted information unit (Iue) with a second decryption system to produce said information unit (Iu) or a second encrypted information unit (Iue).

28. An information transmission system (100) as claimed in Claim 27, further comprising:

a second encryption means (112) for encrypting said multiple information (Im) with a second predetermined encryption system to produce said encrypted multiplexed information (Iue); and
a second multiplex means (113) for multiplexing said encrypted information unit (Iue) to produce said multiplexed information (Im).

29. An information transmission system (100) as claimed in Claim 28, further comprising:

a third encryption means (114) for encrypting said multiplexed information (Im) with a third predetermined encryption system to produce an encrypted multiple information unit (Ime).

30. An information transmission system (500) as claimed in Claim 29, wherein said third predetermined encryption system is the same as that applied to said encrypted information (It).

31. An information transmission system (500) as claimed in Claim 29, wherein said second predetermined encryption system is the same as said third predetermined encryption system.

32. An information transmission system (500) as claimed in Claim 29, wherein said first, second, and third predetermined encryption systems are the same.

33. An information transmission system (100) as claimed in Claim 27, further comprising:

a transmitting means (115) for converting said encrypted multiplexed information (Ime) into a format suitable for an efficient transmission.

34. An information transmission system (500R) as claimed in Claim 27, wherein said first encryption means (512) encrypts said information unit (Iu) with an encryption system suitable for the transmission of information.

35. An information transmission system (100) as claimed in Claim 27, further comprising:

a second demultiplex means (133) for demultiplexing said second multiplexed information unit (Iue);
a third decryption means (132) for decrypting said second encrypted information unit (Iue) with a third predetermined decryption system to produce said information unit (Iu).

36. An information transmission system (100) as claimed in Claim 27, wherein said first decryption system is the same as that applied to said encrypted information (It).

37. An information transmission system apparatus (1000) as claimed in Claim 27, further comprising:

a storage means (1034) provided between said first demultiplexing means (1033) and said second decryption means (1035) for storing any of said first and second encrypted information units (Iue).

38. An information transmission system (1000) as claimed in Claim 30, further comprising:

a reproducing means (1036) for receiving said encrypted information units (Iue) from said second decryption means (1035) to produce a reproduction information (Ir) indicating a content said encrypted information (It), said reproducing means (1036) requesting said storage means (1034) to supply said stored encryption information unit (Iue) to said second decryption means (1035).

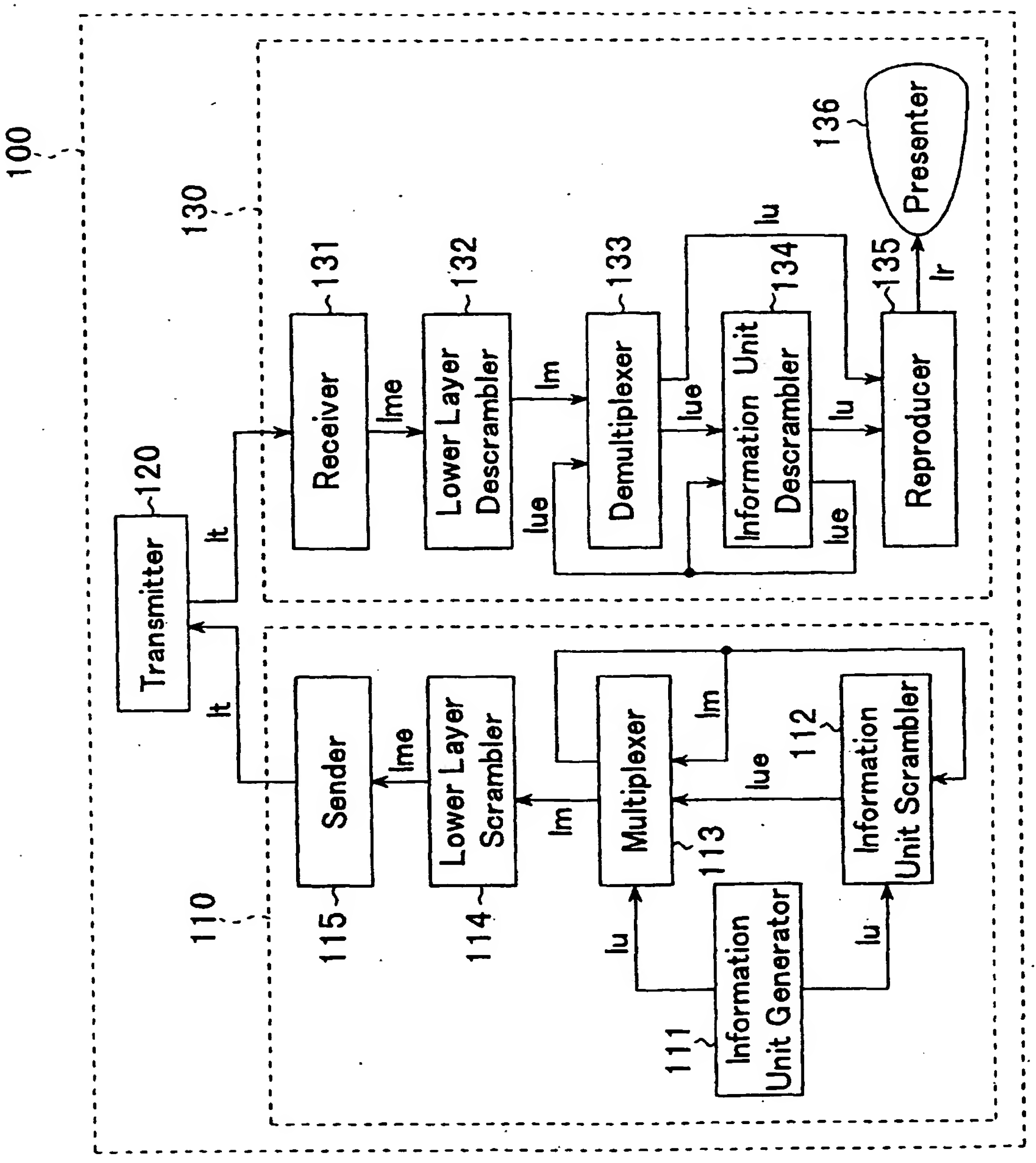

100
110
130
Transmitter
120
It
It
Receiver
131
Ime
Lower Layer Descrambler
132
Im
Demultiplexer
133
Iue
Iue
Iue
Information Unit Descrambler
134
Iu
Iu
Reproducer
135
Ir
Presenter
136
Sender
115
Ime
Lower Layer Scrambler
114
Im
Multiplexer
113
Im
Iue
Information Unit Scrambler
112
Iu
Iu
Information Unit Generator
111

Fig. 1

Fig. 2

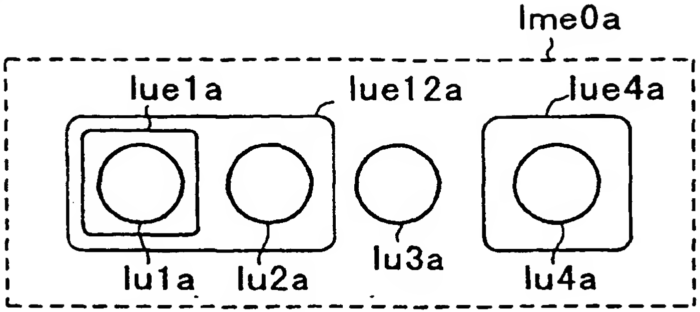


Fig. 6

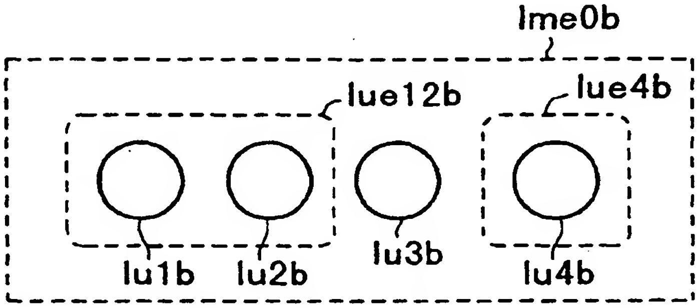


Fig. 11

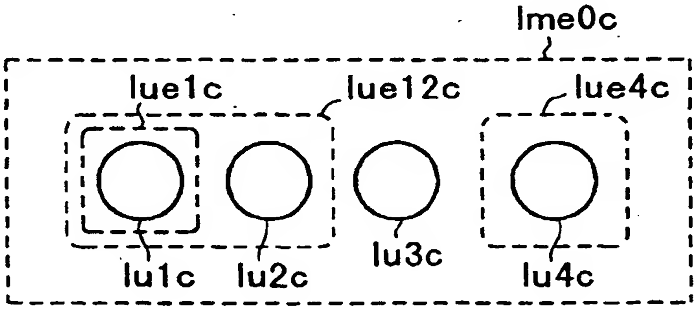


Fig. 26

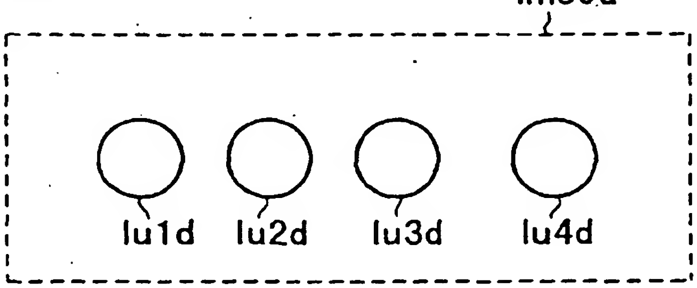


Fig. 3

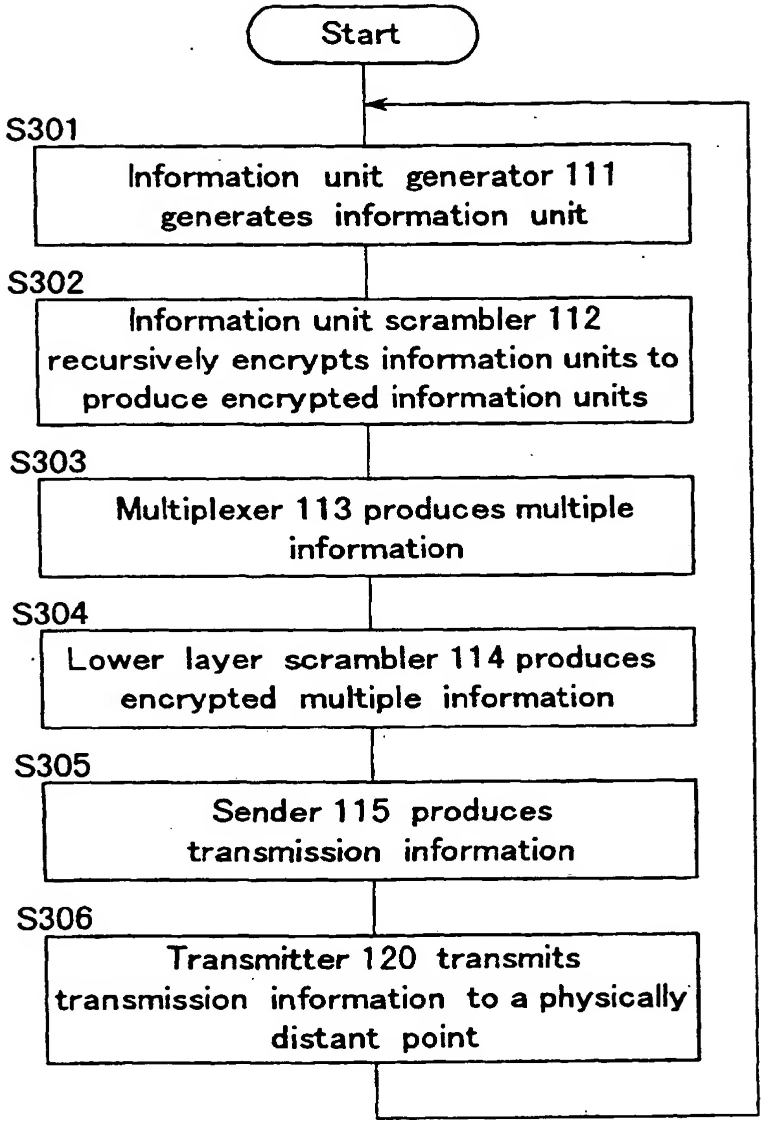

Start
S301
Information unit generator 111 generates information unit
S302
Information unit scrambler 112 recursively encrypts information units to produce encrypted information units
S303
Multiplexer 113 produces multiple information
S304
Lower layer scrambler 114 produces encrypted multiple information
S305
Sender 115 produces transmission information
S306
Transmitter 120 transmits transmission information to a physically distant point

Fig. 4

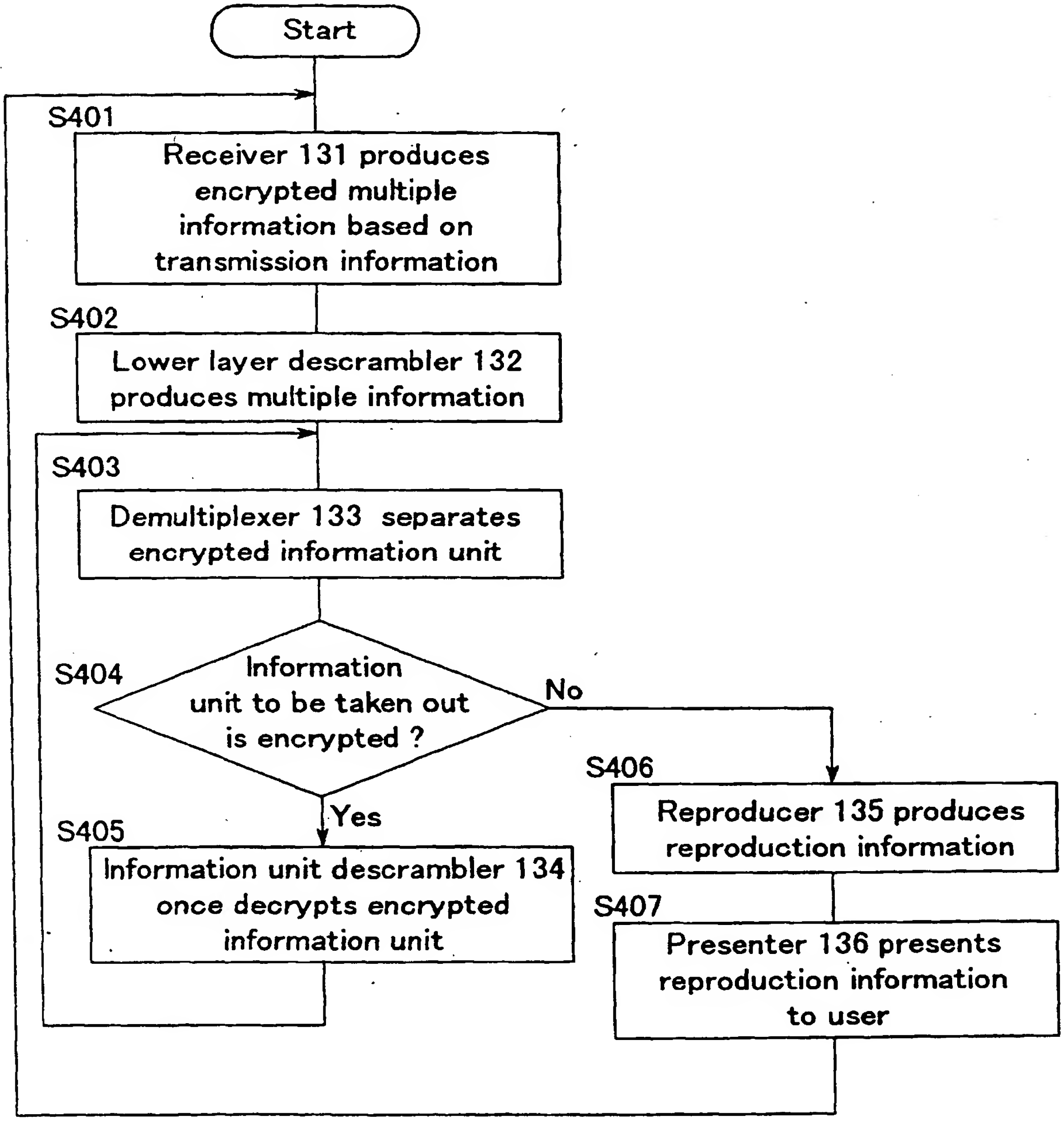

Start
S401
Receiver 131 produces encrypted multiple information based on transmission information
S402
Lower layer descrambler 132 produces multiple information
S403
Demultiplexer 133 separates encrypted information unit
S404
Information unit to be taken out is encrypted ?
No
Yes
S405
Information unit descrambler 134 once decrypts encrypted information unit
S406
Reproducer 135 produces reproduction information
S407
Presenter 136 presents reproduction information to user

Fig. 5

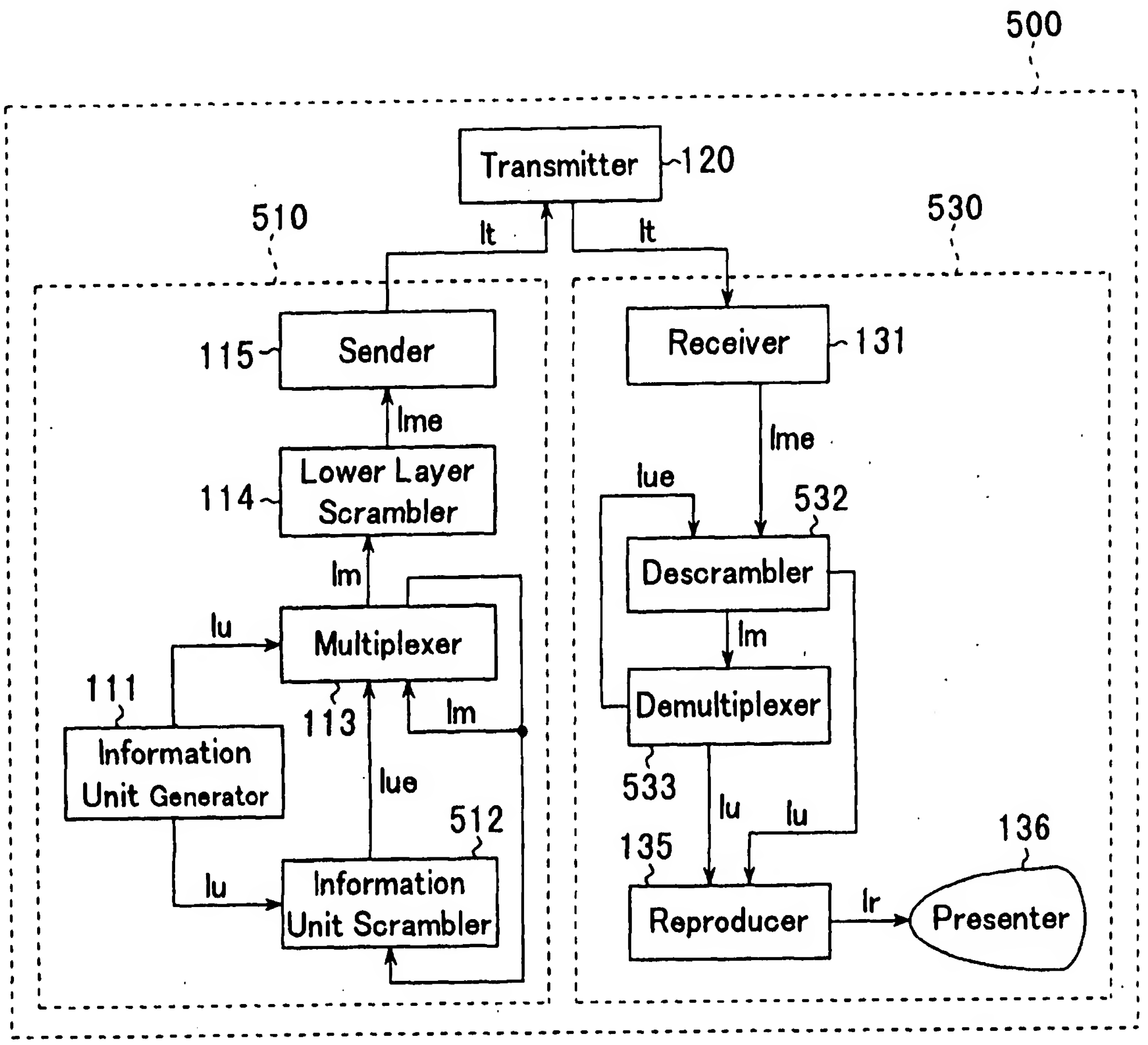

500
Transmitter
120
It
It
510
530
Sender
115
Receiver
131
Ime
Ime
Lower Layer Scrambler
114
Iue
532
Descrambler
Im
Im
Multiplexer
Im
111
113
Im
Demultiplexer
Information Unit Generator
Iue
533
512
Iu
Iu
135
136
Iu
Iu
Information Unit Scrambler
Reproducer
Ir
Presenter

Fig. 7

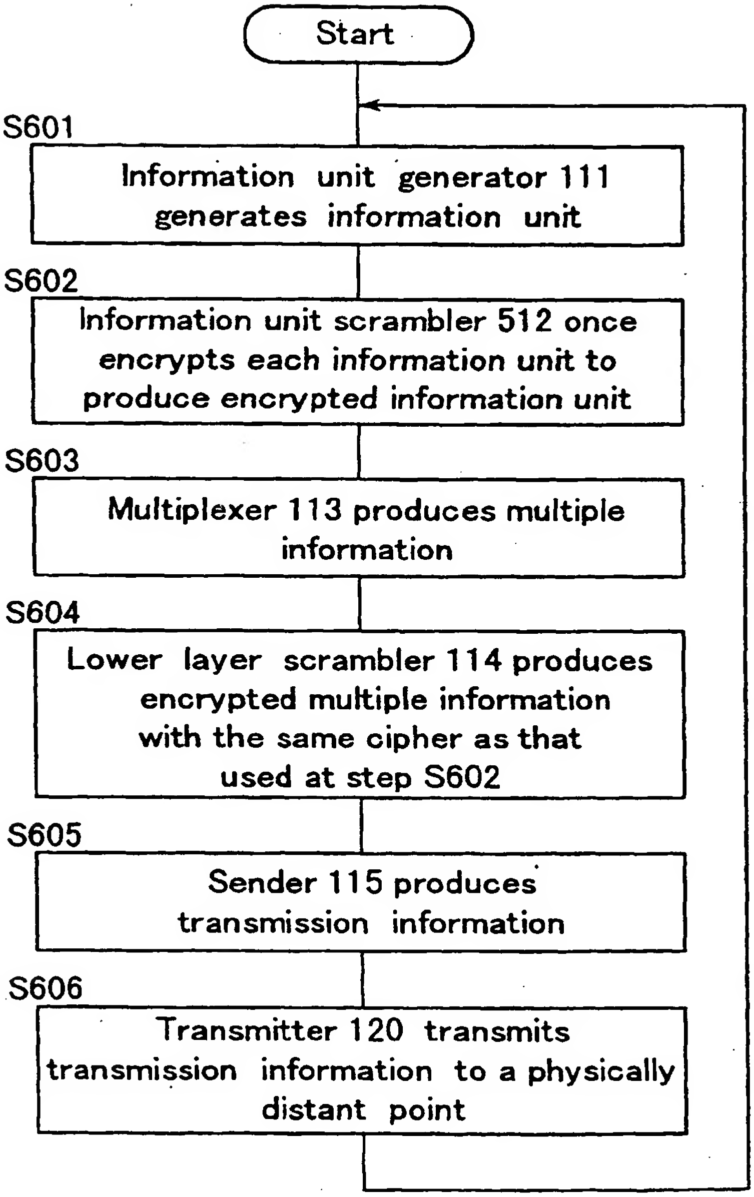
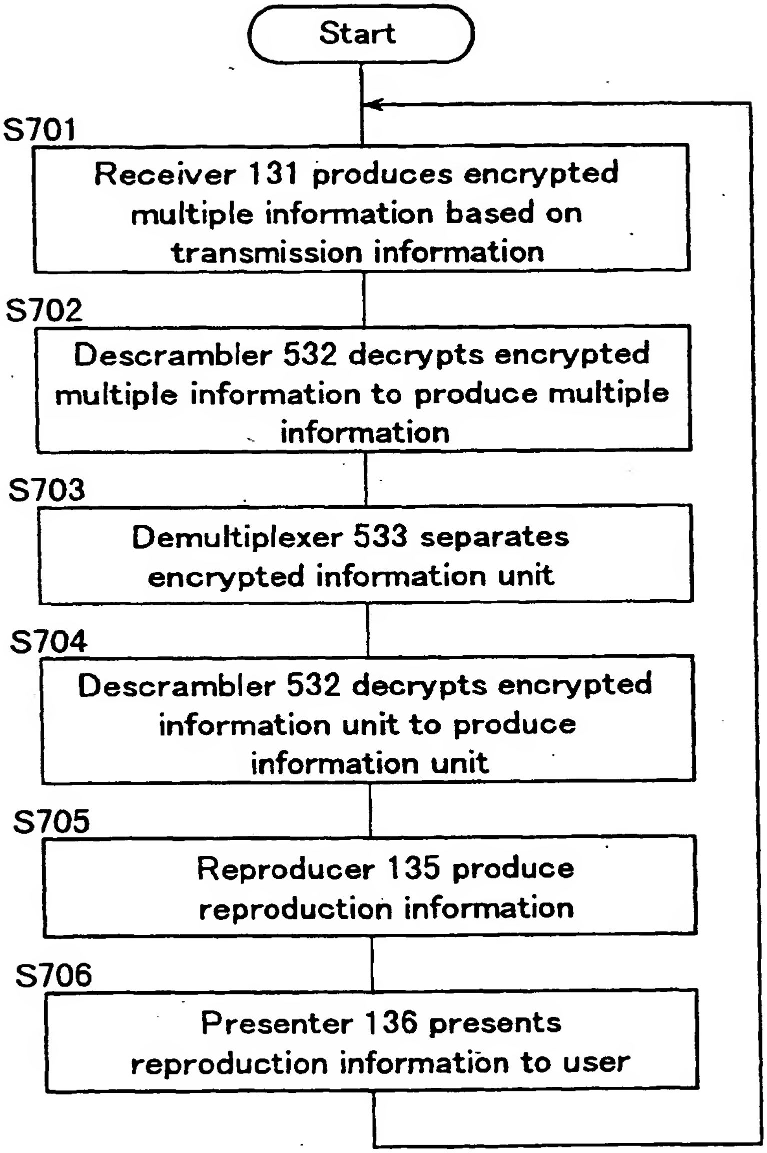

Start
S601
Information unit generator 111 generates information unit
S602
Information unit scrambler 512 once encrypts each information unit to produce encrypted information unit
S603
Multiplexer 113 produces multiple information
S604
Lower layer scrambler 114 produces encrypted multiple information with the same cipher as that used at step S602
S605
Sender 115 produces transmission information
S606
Transmitter 120 transmits transmission information to a physically distant point

Fig. 8


Start
S701
Receiver 131 produces encrypted multiple information based on transmission information
S702
Descrambler 532 decrypts encrypted multiple information to produce multiple information
S703
Demultiplexer 533 separates encrypted information unit
S704
Descrambler 532 decrypts encrypted information unit to produce information unit
S705
Reproducer 135 produce reproduction information
S706
Presenter 136 presents reproduction information to user

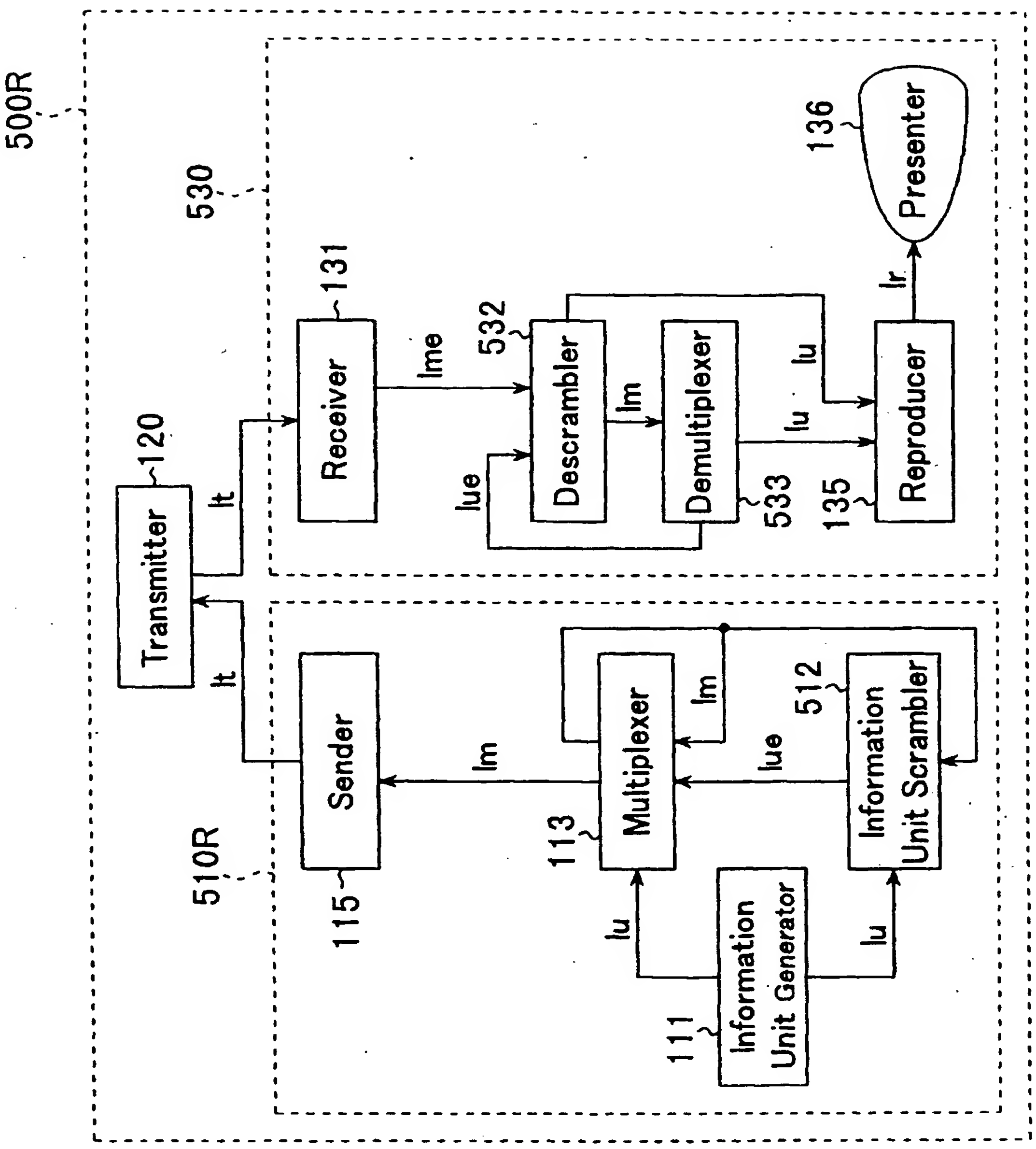

500R
510R
530
Transmitter
120
It
It
Receiver
131
Ime
Descrambler
532
Im
Demultiplexer
533
Iue
Iu
Iu
Reproducer
135
Ir
Presenter
136
Sender
115
Im
Multiplexer
113
Im
Iue
Information Unit Scrambler
512
Iu
Iu
Information Unit Generator
111

Fig. 9

Fig. 10

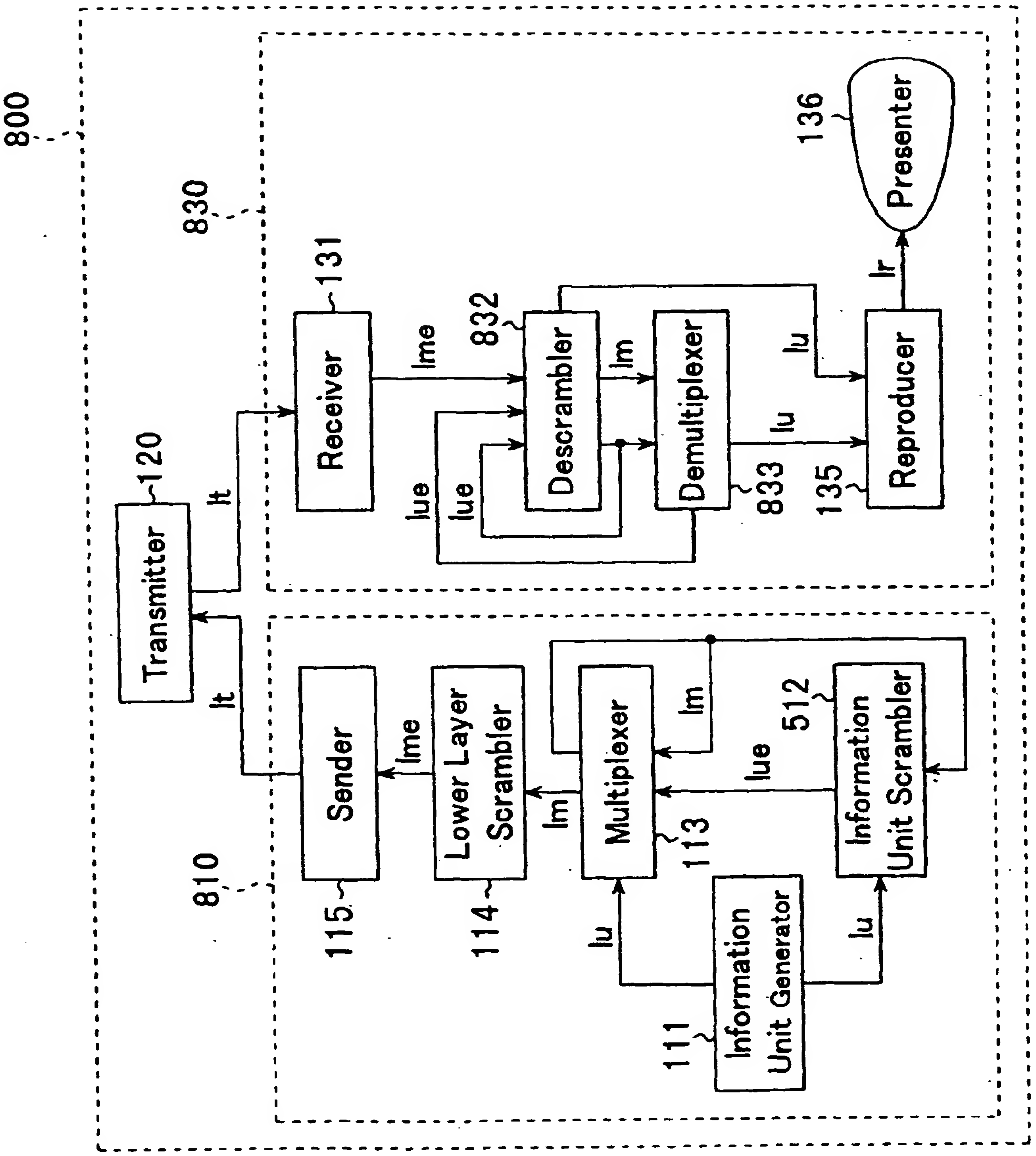
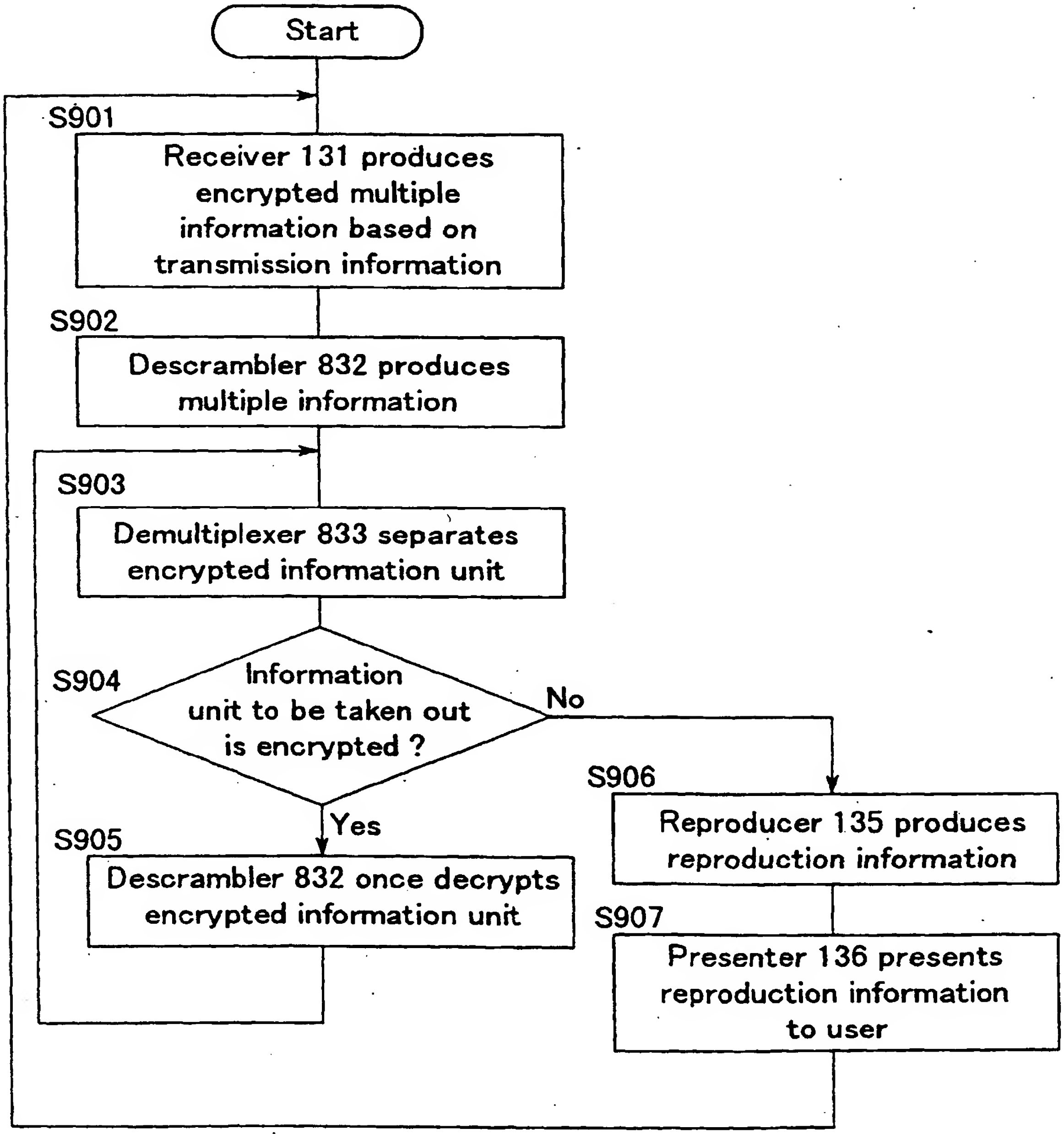

800
830
810
Transmitter
120
It
It
Receiver
131
Ime
832
Descrambler
Im
Demultiplexer
Iue
Iue
833
Iu
Iu
Reproducer
135
Ir
Presenter
136
Sender
115
Ime
Lower Layer Scrambler
114
Im
Multiplexer
113
Im
Iue
Information Unit Scrambler
512
Iu
Iu
Information Unit Generator
111

Fig. 12


Start
S901
Receiver 131 produces encrypted multiple information based on transmission information
S902
Descrambler 832 produces multiple information
S903
Demultiplexer 833 separates encrypted information unit
S904
Information unit to be taken out is encrypted ?
No
Yes
S905
Descrambler 832 once decrypts encrypted information unit
S906
Reproducer 135 produces reproduction information
S907
Presenter 136 presents reproduction information to user

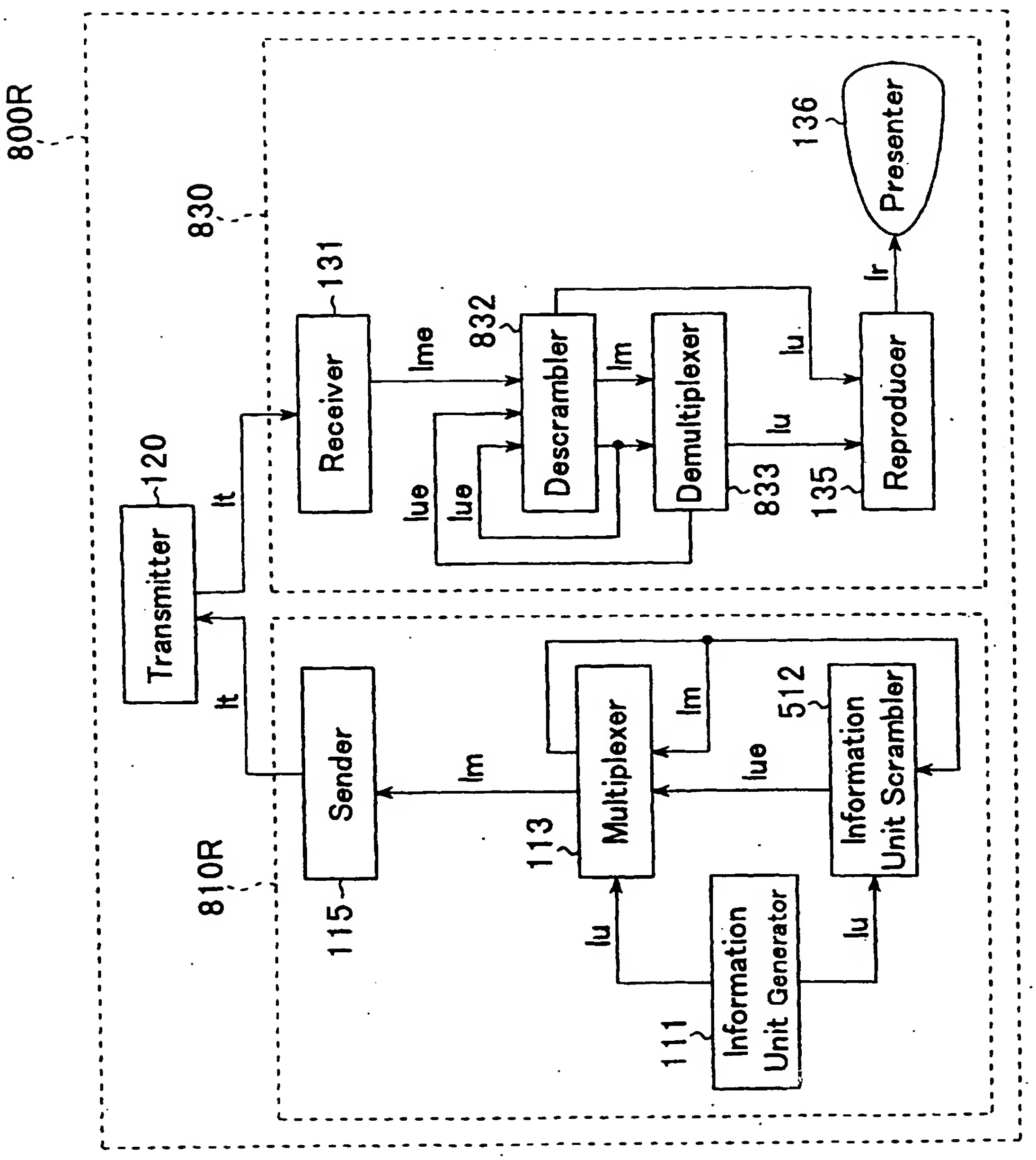

800R
830
136
Presenter
131
Receiver
Ime
832
Descrambler
Im
Demultiplexer
Iu
Ir
Reproducer
Iu
Iue
Iue
833
135
120
Transmitter
It
It
Sender
810R
115
Im
113
Multiplexer
Im
Iue
512
Information Unit Scrambler
Iu
Iu
111
Information Unit Generator

Fig. 13

Fig. 14

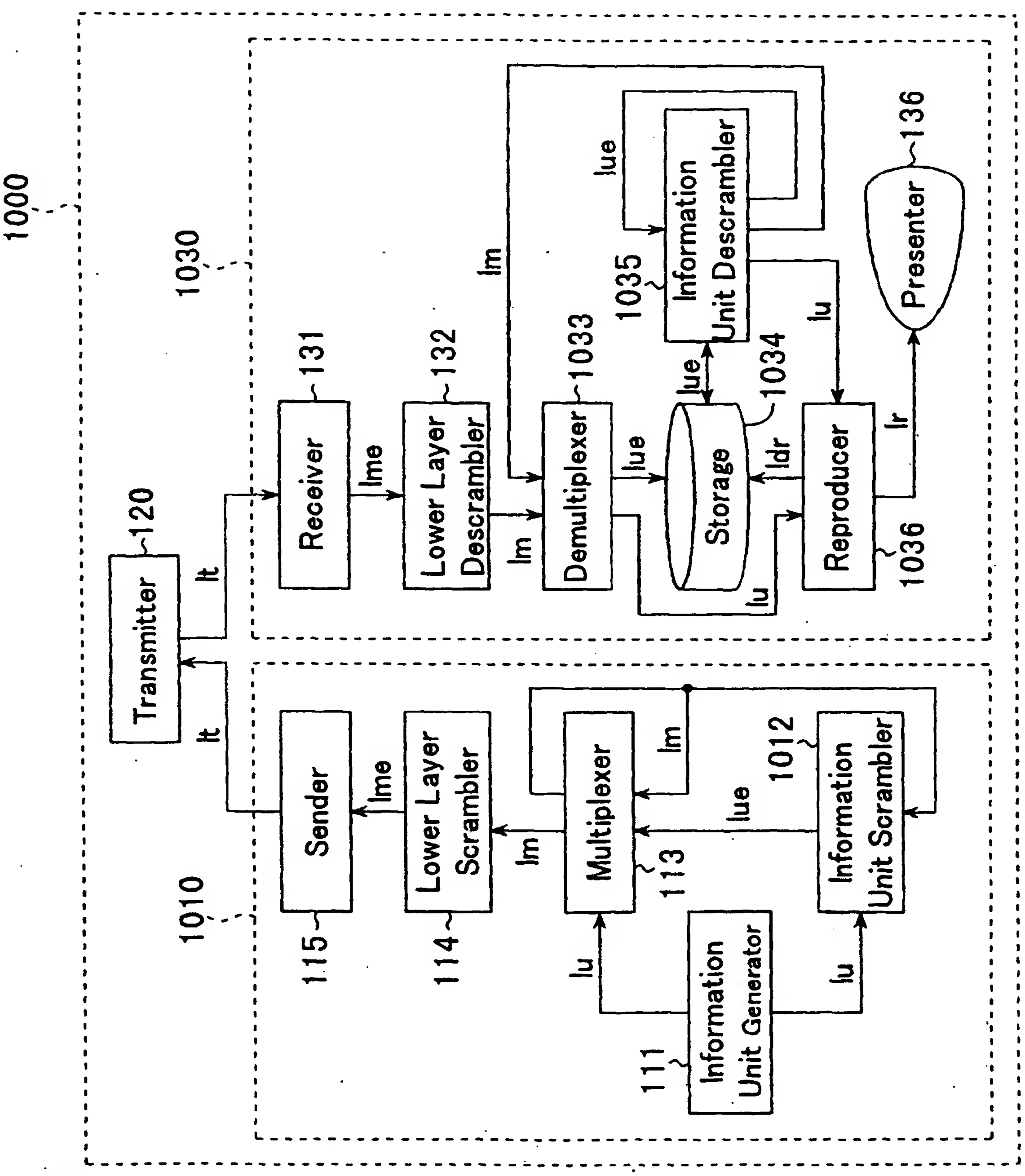

1000
1010
1030
Transmitter
120
It
It
Receiver
131
Ime
Lower Layer Descrambler
132
Im
Demultiplexer
1033
Im
Iue
Iu
Storage
1034
Iue
Information Unit Descrambler
1035
Iue
Iu
Idr
Reproducer
1036
Ir
Presenter
136
Sender
115
Ime
Lower Layer Scrambler
114
Im
Multiplexer
113
Im
Iue
Information Unit Scrambler
1012
Iu
Iu
Information Unit Generator
111

Fig. 15

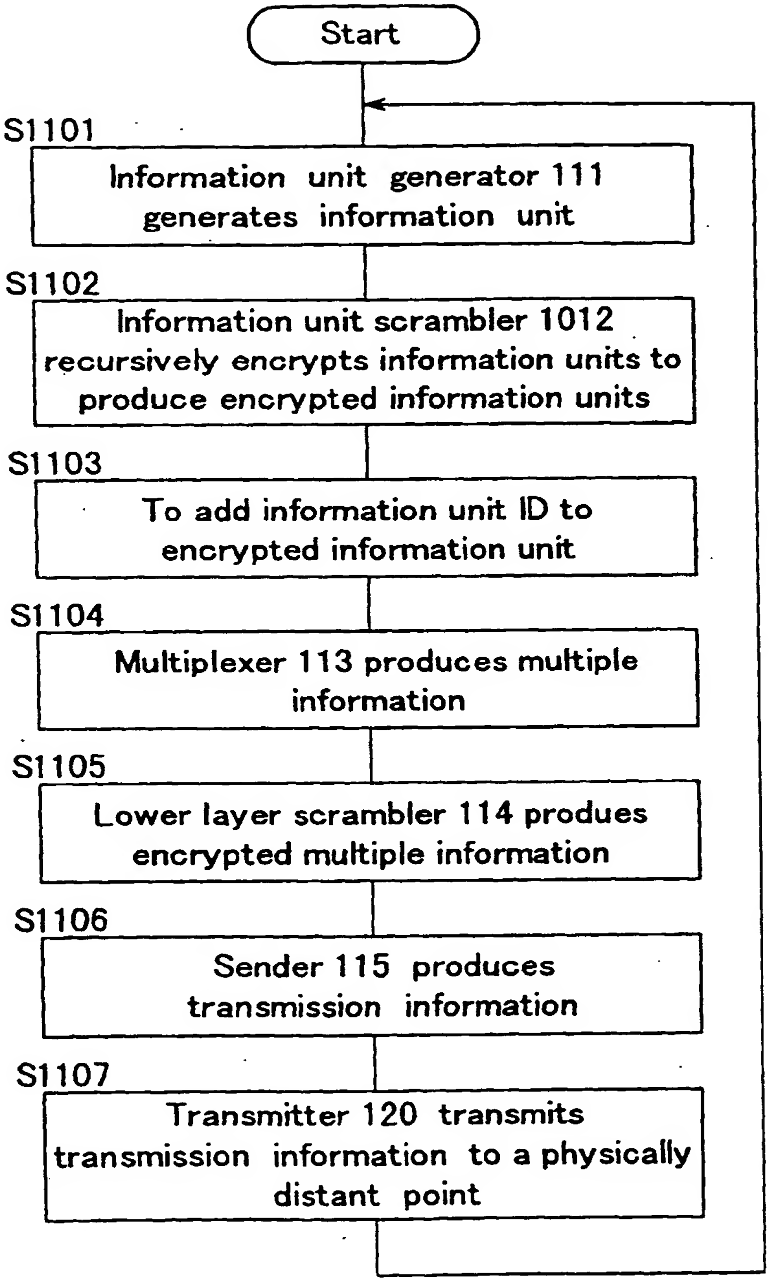

Start
S1101
Information unit generator 111 generates information unit
S1102
Information unit scrambler 1012 recursively encrypts information units to produce encrypted information units
S1103
To add information unit ID to encrypted information unit
S1104
Multiplexer 113 produces multiple information
S1105
Lower layer scrambler 114 produes encrypted multiple information
S1106
Sender 115 produces transmission information
S1107
Transmitter 120 transmits transmission information to a physically distant point

Fig. 16

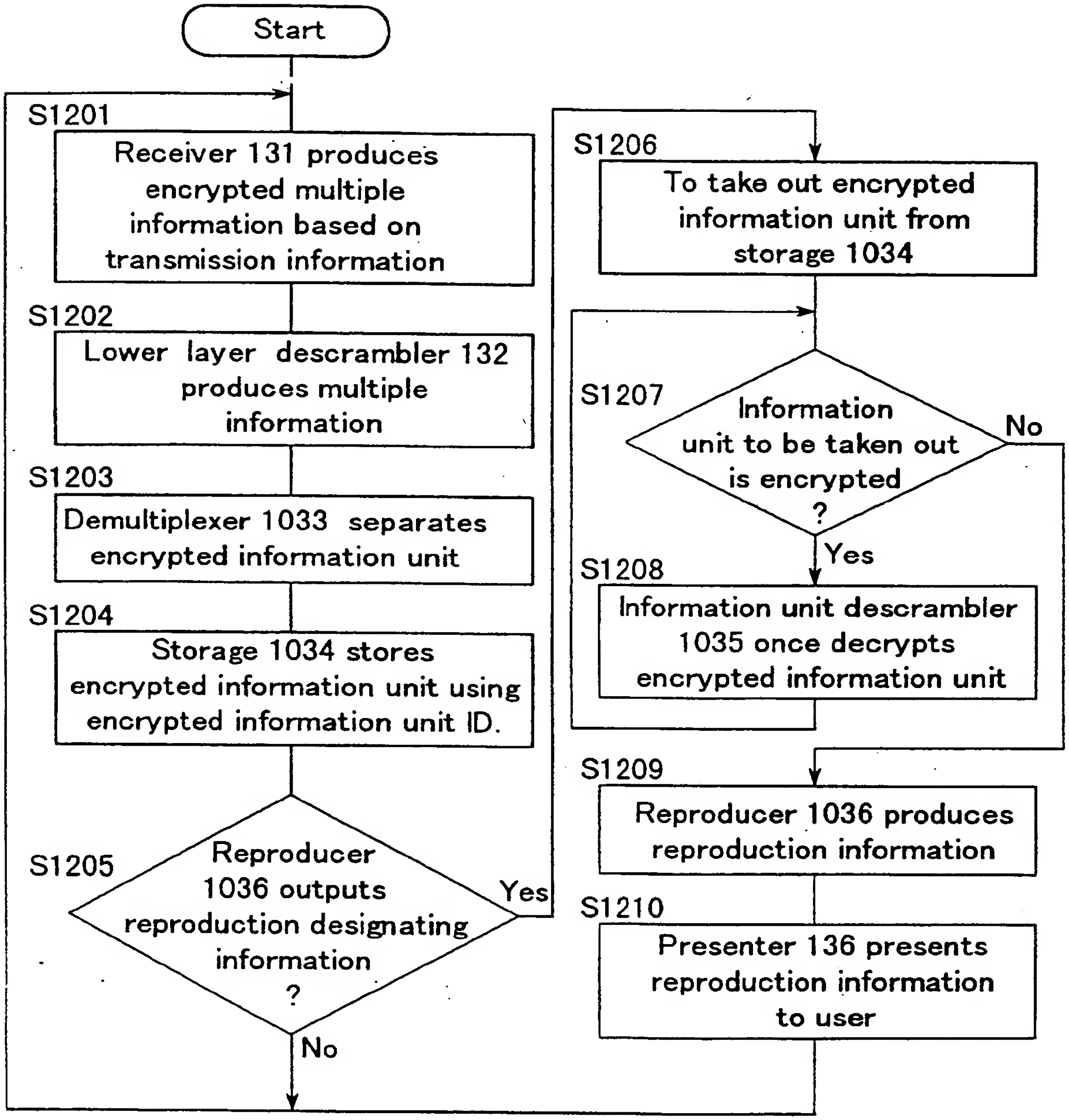

Start
S1201
Receiver 131 produces encrypted multiple information based on transmission information
S1202
Lower layer descrambler 132 produces multiple information
S1203
Demultiplexer 1033 separates encrypted information unit
S1204
Storage 1034 stores encrypted information unit using encrypted information unit ID.
S1205
Reproducer 1036 outputs reproduction designating information ?
Yes
No
S1206
To take out encrypted information unit from storage 1034
S1207
Information unit to be taken out is encrypted ?
No
Yes
S1208
Information unit descrambler 1035 once decrypts encrypted information unit
S1209
Reproducer 1036 produces reproduction information
S1210
Presenter 136 presents reproduction information to user

Fig. 17

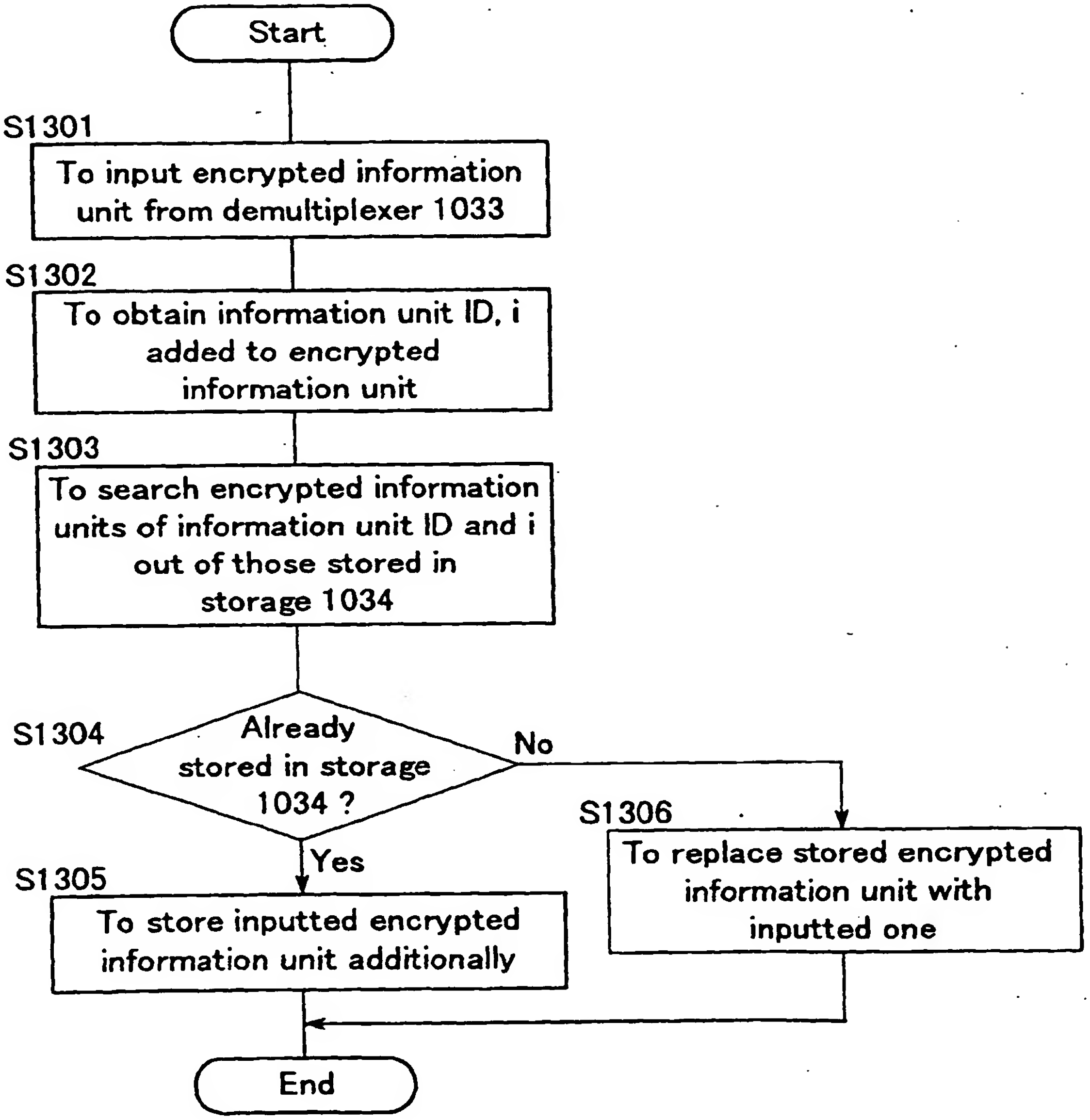

Start
S1301
To input encrypted information unit from demultiplexer 1033
S1302
To obtain information unit ID, i added to encrypted information unit
S1303
To search encrypted information units of information unit ID and i out of those stored in storage 1034
S1304
Already stored in storage 1034 ?
No
Yes
S1305
To store inputted encrypted information unit additionally
S1306
To replace stored encrypted information unit with inputted one
End

Fig. 18

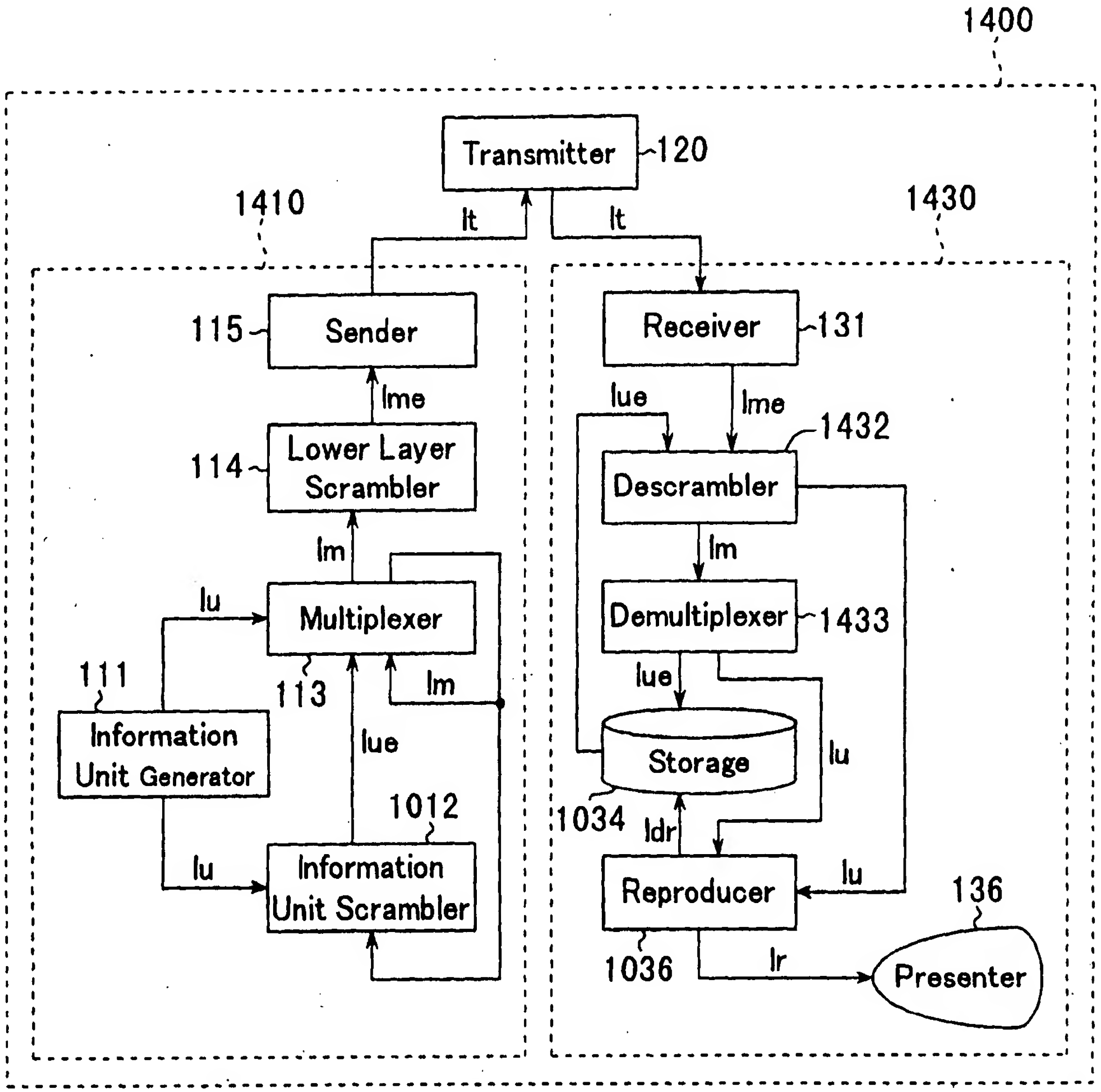

1400
Transmitter
120
It
It
1410
1430
115
Sender
Receiver
131
Ime
lue
Ime
114
Lower Layer Scrambler
1432
Descrambler
Im
Im
Iu
Multiplexer
Demultiplexer
1433
111
113
Im
lue
Information Unit Generator
lue
Storage
Iu
1012
1034
Idr
Iu
Information Unit Scrambler
Reproducer
Iu
136
1036
Ir
Presenter

Fig. 19

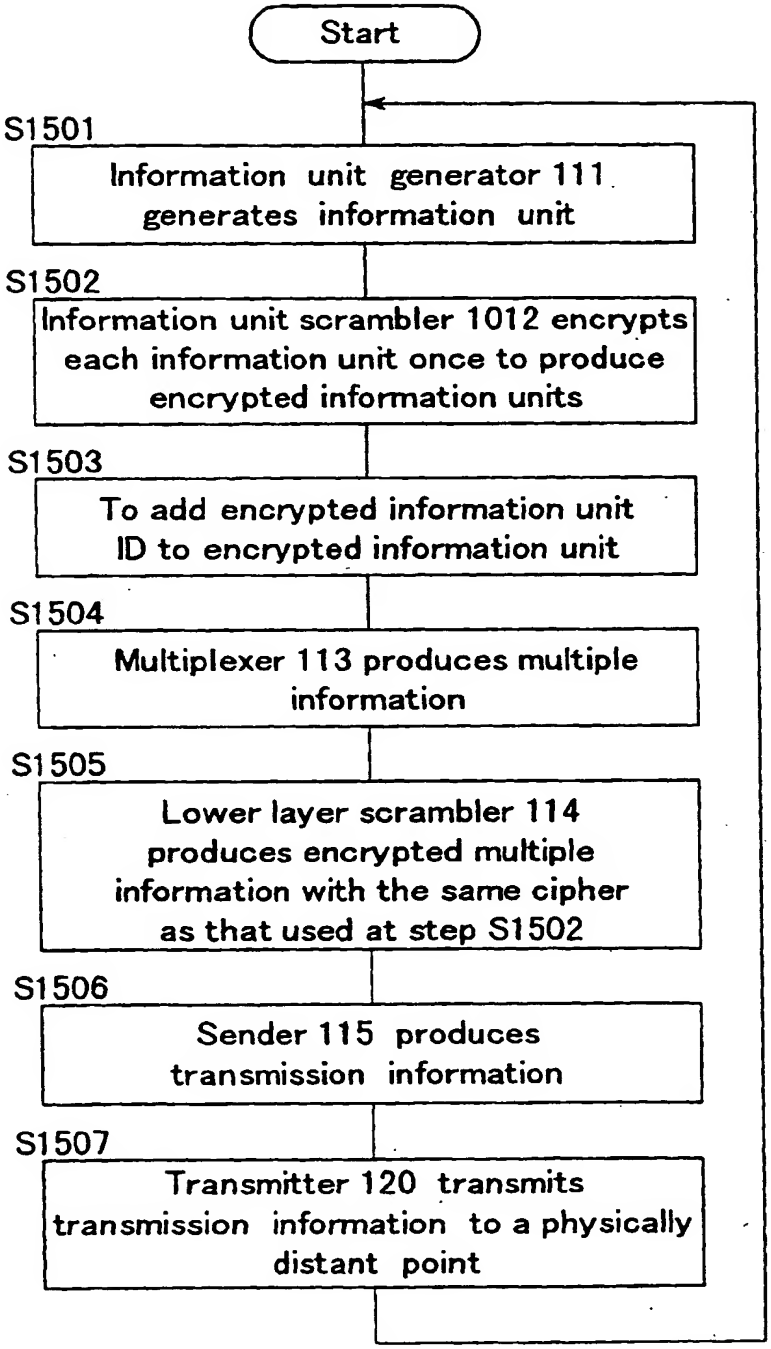

Start
S1501
Information unit generator 111 generates information unit
S1502
Information unit scrambler 1012 encrypts each information unit once to produce encrypted information units
S1503
To add encrypted information unit ID to encrypted information unit
S1504
Multiplexer 113 produces multiple information
S1505
Lower layer scrambler 114 produces encrypted multiple information with the same cipher as that used at step S1502
S1506
Sender 115 produces transmission information
S1507
Transmitter 120 transmits transmission information to a physically distant point

Fig. 20

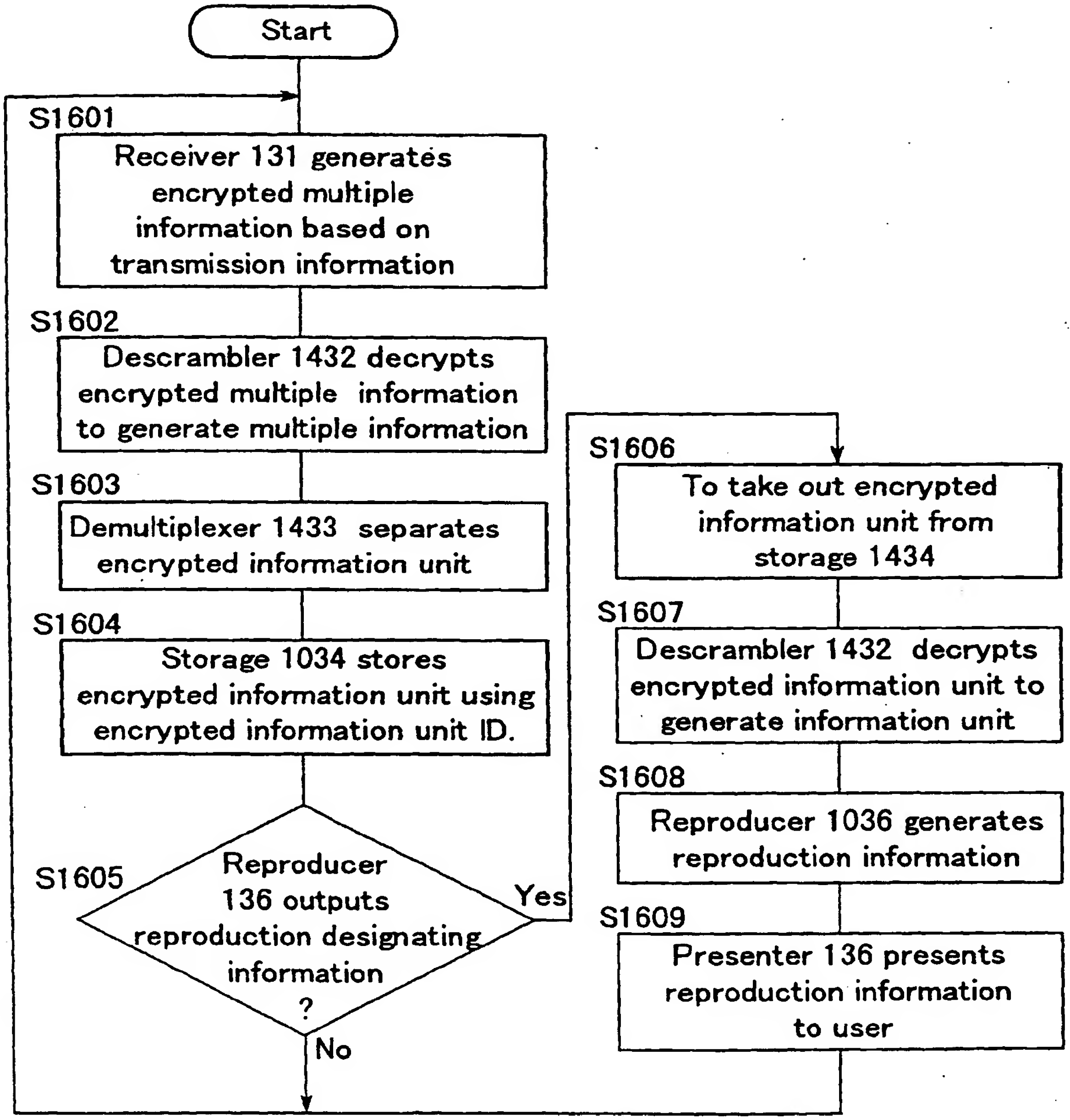
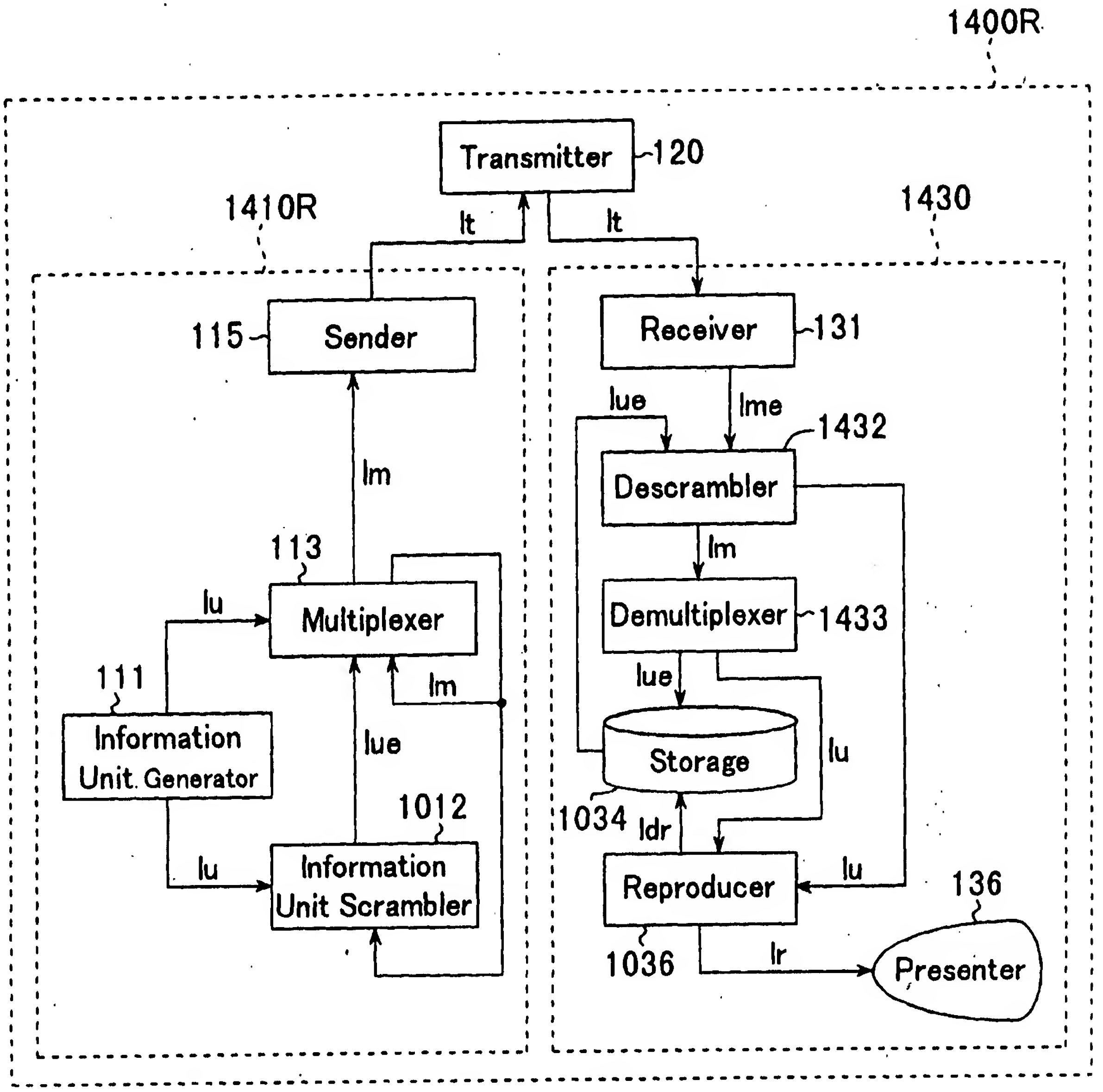

Start
S1601
Receiver 131 generates encrypted multiple information based on transmission information
S1602
Descrambler 1432 decrypts encrypted multiple information to generate multiple information
S1603
Demultiplexer 1433 separates encrypted information unit
S1604
Storage 1034 stores encrypted information unit using encrypted information unit ID.
S1605
Reproducer 136 outputs reproduction designating information ?
Yes
No
S1606
To take out encrypted information unit from storage 1434
S1607
Descrambler 1432 decrypts encrypted information unit to generate information unit
S1608
Reproducer 1036 generates reproduction information
S1609
Presenter 136 presents reproduction information to user

Fig. 21


1400R
Transmitter
120
1410R
It
It
1430
115
Sender
Receiver
131
Iue
Ime
1432
Descrambler
Im
Im
113
Multiplexer
Demultiplexer
1433
Iu
111
Im
Iue
Information
Unit. Generator
Iue
Storage
Iu
1012
1034
Idr
Iu
Information
Unit Scrambler
Reproducer
Iu
136
1036
Ir
Presenter

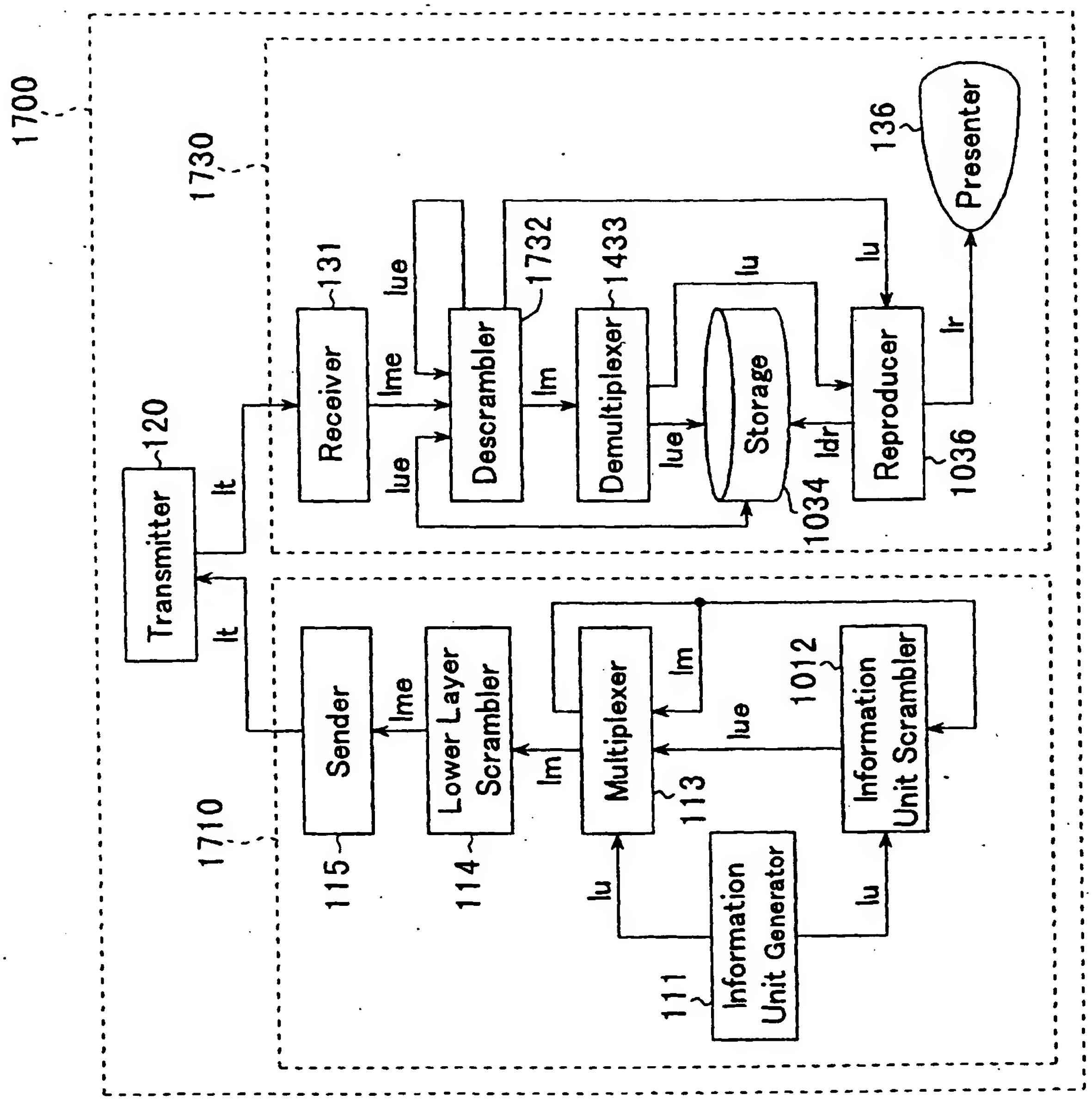

1700
1730
1710
Transmitter
120
It
It
Receiver
131
Ime
Iue
Iue
Descrambler
1732
Im
Demultiplexer
1433
Iue
Iu
Iu
Storage
1034
Idr
Reproducer
1036
Ir
Presenter
136
Sender
115
Ime
Lower Layer Scrambler
114
Im
Multiplexer
113
Im
Iue
Information Unit Scrambler
1012
Iu
Iu
Information Unit Generator
111

Fig. 22

Fig. 23

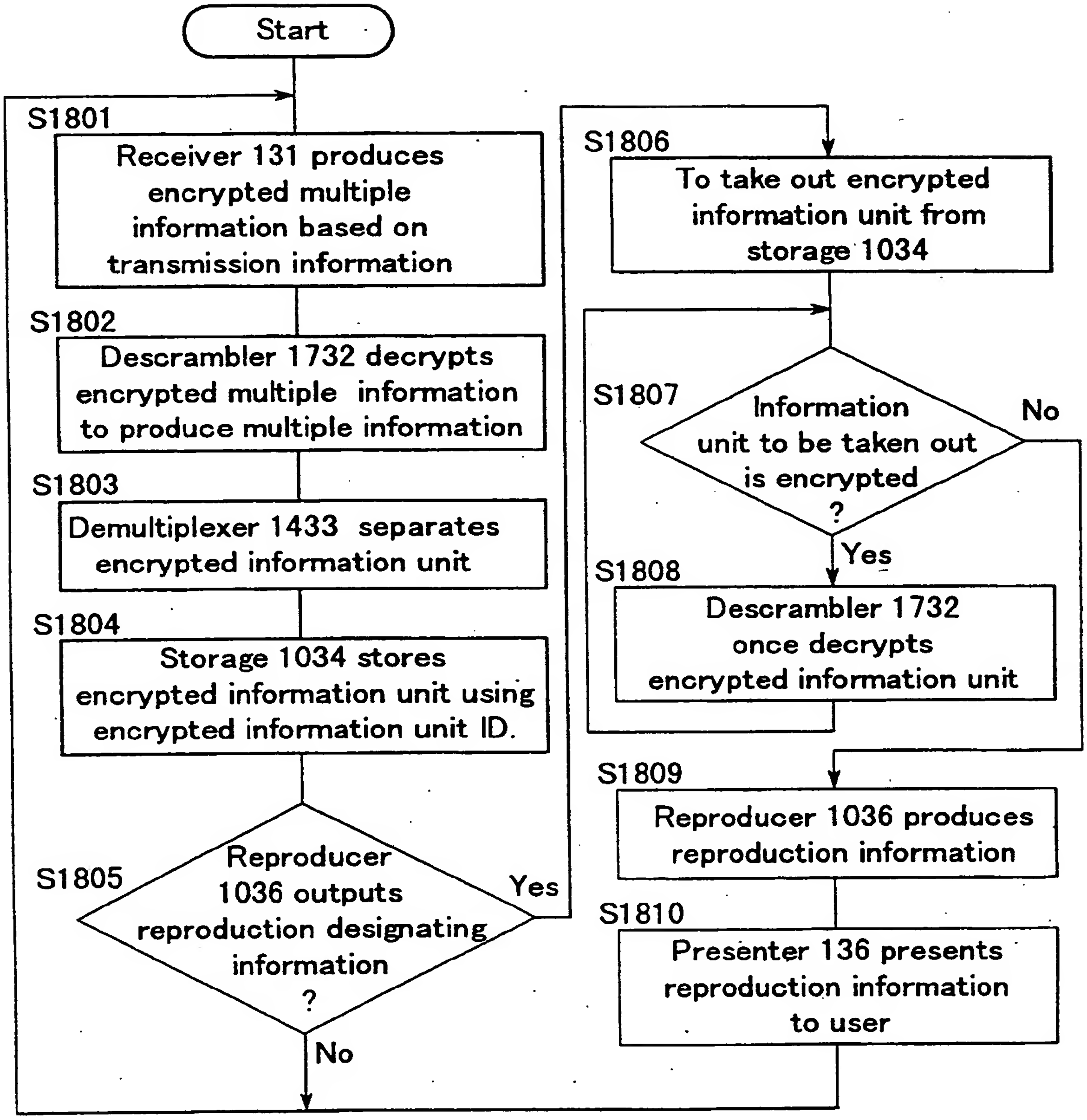

Start
S1801
Receiver 131 produces encrypted multiple information based on transmission information
S1802
Descrambler 1732 decrypts encrypted multiple information to produce multiple information
S1803
Demultiplexer 1433 separates encrypted information unit
S1804
Storage 1034 stores encrypted information unit using encrypted information unit ID.
S1805
Reproducer 1036 outputs reproduction designating information ?
Yes
No
S1806
To take out encrypted information unit from storage 1034
S1807
Information unit to be taken out is encrypted ?
No
Yes
S1808
Descrambler 1732 once decrypts encrypted information unit
S1809
Reproducer 1036 produces reproduction information
S1810
Presenter 136 presents reproduction information to user

Fig. 24

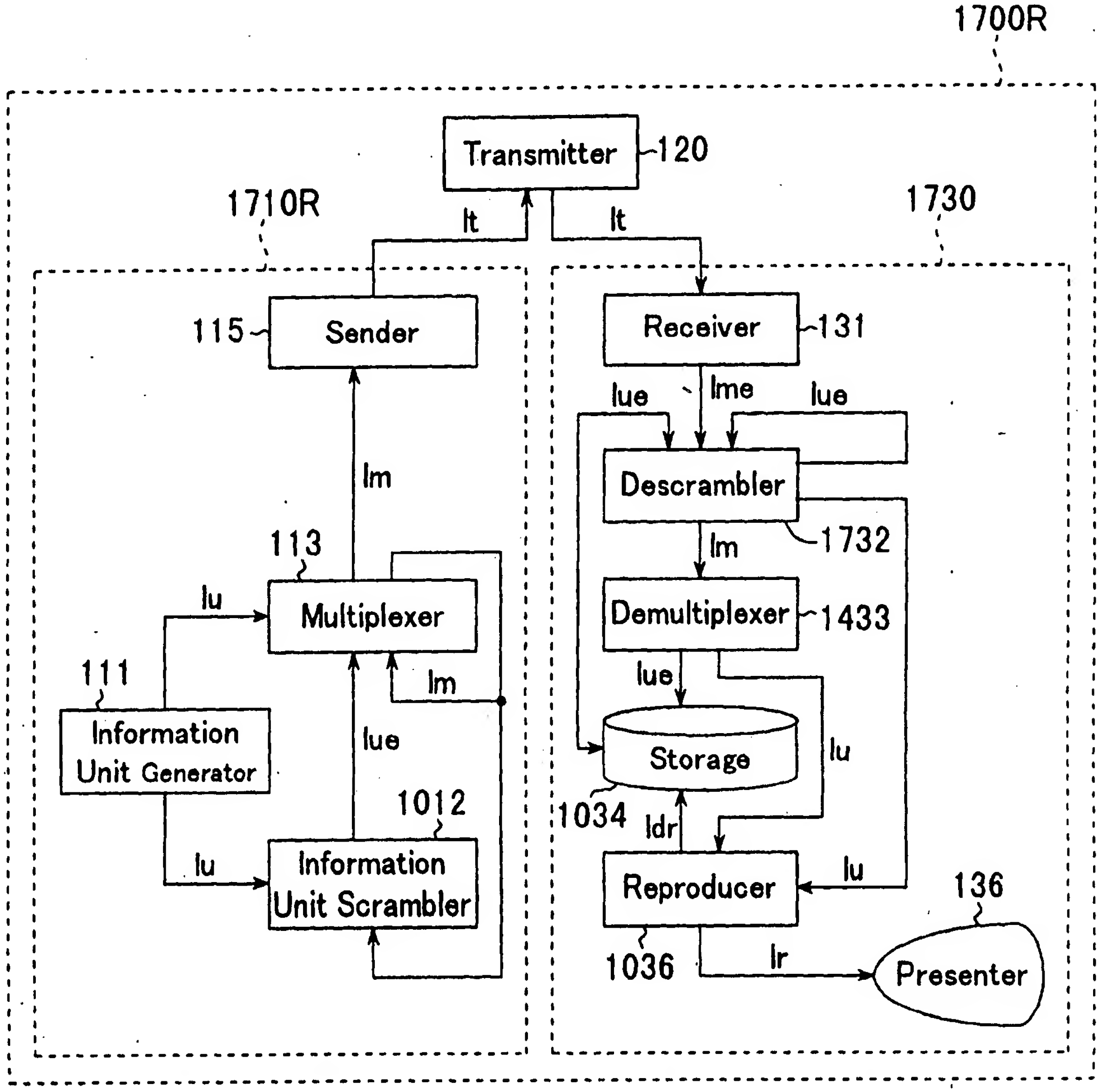

1700R
Transmitter
120
1710R
It
It
1730
115
Sender
Receiver
131
Iue
Ime
Iue
Im
Descrambler
1732
113
Im
Iu
Multiplexer
Demultiplexer
1433
111
Im
Iue
Information
Unit Generator
Iue
Storage
Iu
1012
1034
Idr
Iu
Information
Unit Scrambler
Reproducer
Iu
136
1036
Ir
Presenter

Fig. 25

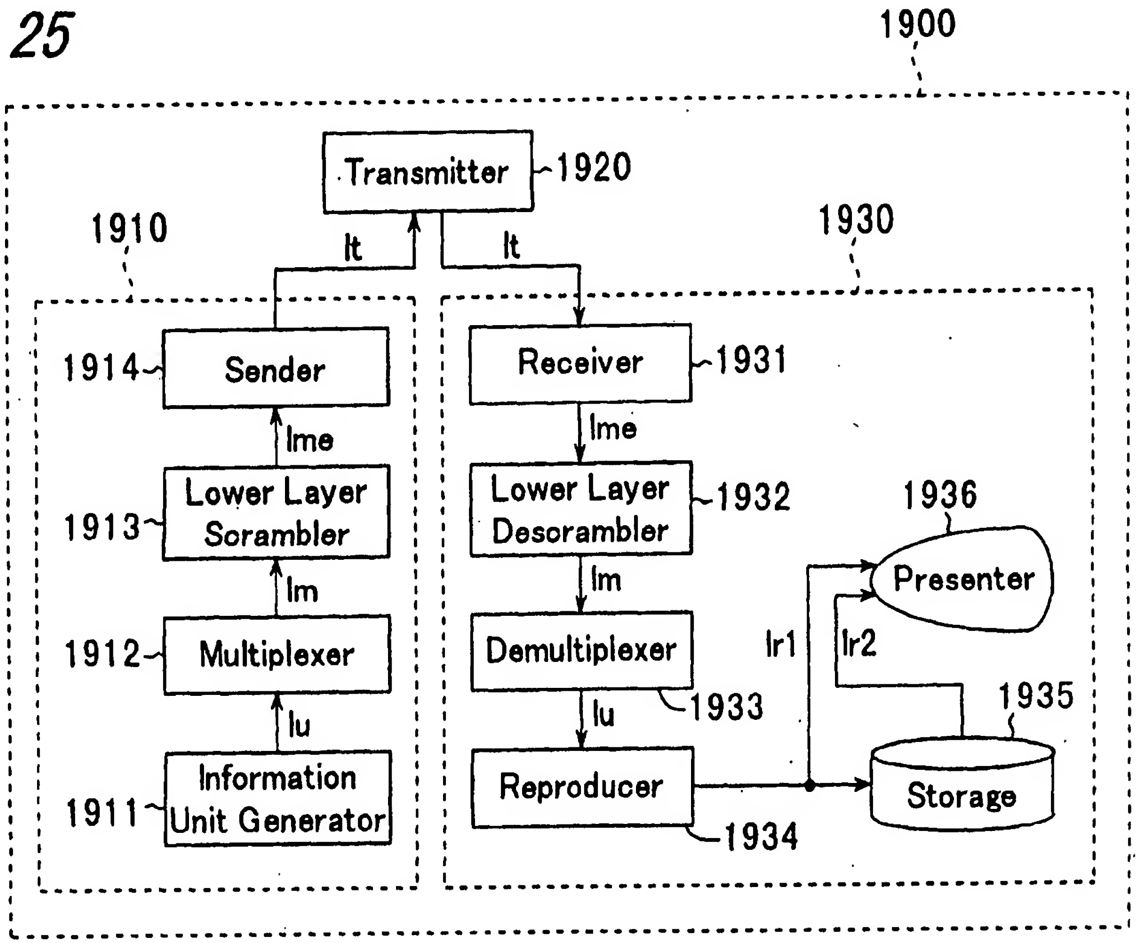

1900
Transmitter
1920
1910
It
It
1930
1914
Sender
Receiver
1931
Ime
Ime
Lower Layer Sorambler
1913
Lower Layer Desorambler
1932
1936
Im
Im
Presenter
1912
Multiplexer
Demultiplexer
Ir1
Ir2
1933
1935
Iu
Iu
1911
Information Unit Generator
Reproducer
Storage
1934

Fig. 27

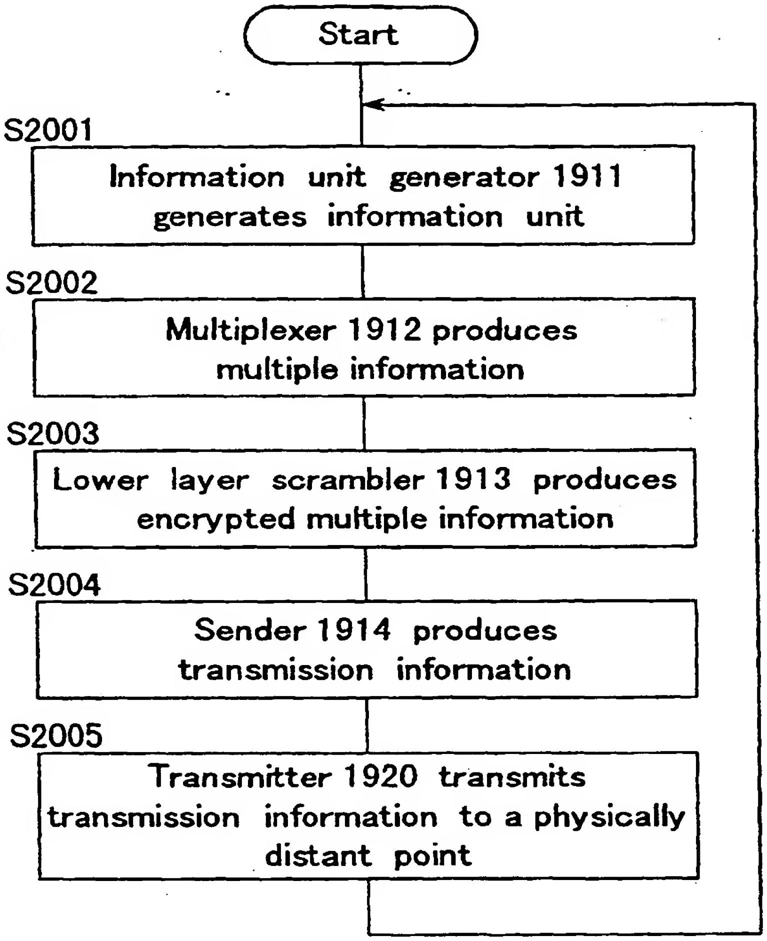
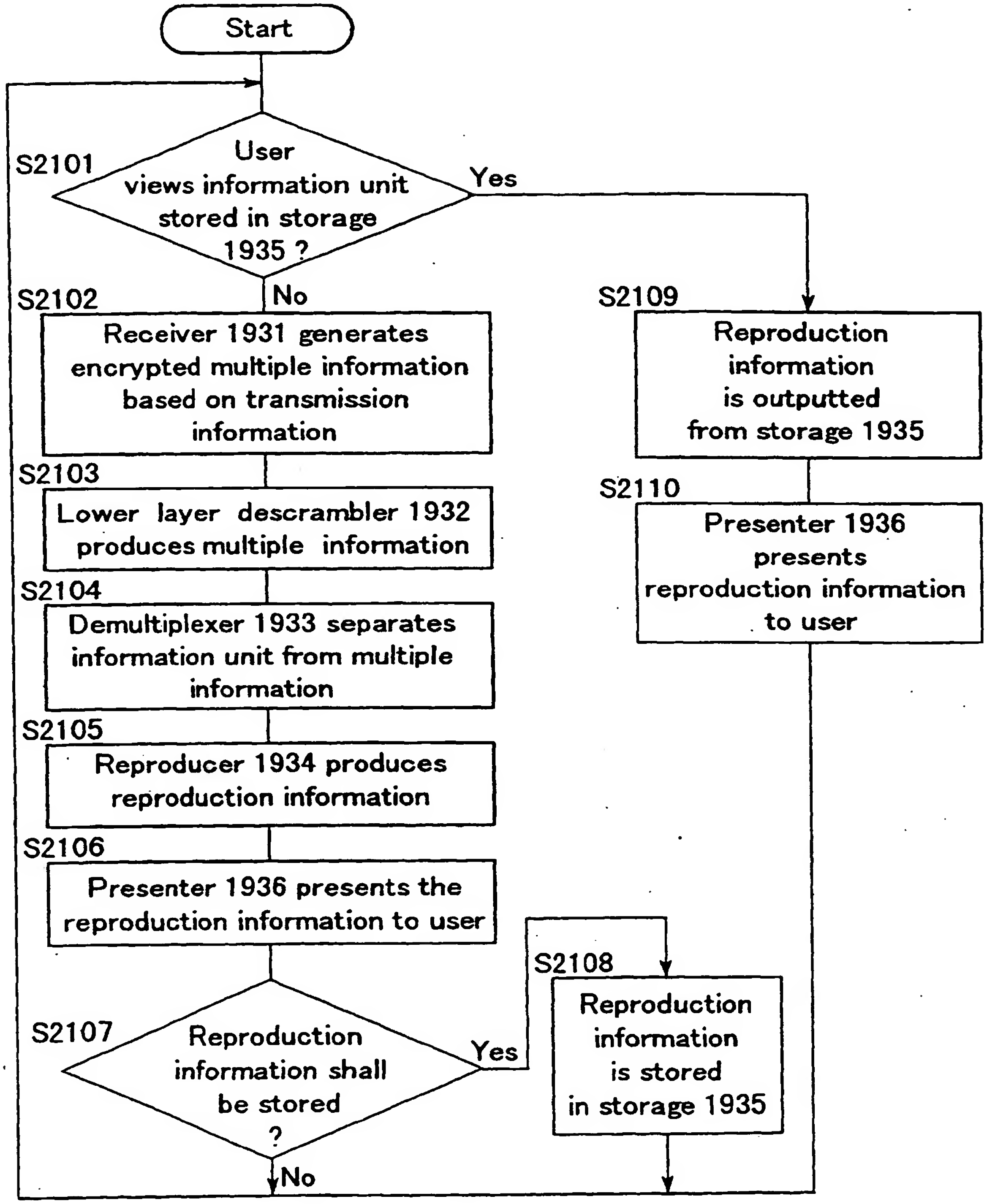

Start
S2001
Information unit generator 1911 generates information unit
S2002
Multiplexer 1912 produces multiple information
S2003
Lower layer scrambler 1913 produces encrypted multiple information
S2004
Sender 1914 produces transmission information
S2005
Transmitter 1920 transmits transmission information to a physically distant point

Fig. 28


Start
S2101
User views information unit stored in storage 1935 ?
Yes
No
S2102
Receiver 1931 generates encrypted multiple information based on transmission information
S2103
Lower layer descrambler 1932 produces multiple information
S2104
Demultiplexer 1933 separates information unit from multiple information
S2105
Reproducer 1934 produces reproduction information
S2106
Presenter 1936 presents the reproduction information to user
S2107
Reproduction information shall be stored ?
Yes
No
S2108
Reproduction information is stored in storage 1935
S2109
Reproduction information is outputted from storage 1935
S2110
Presenter 1936 presents reproduction information to user